



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2014-03

REAL ID and the security of state identity
documents: the long, rocky, and incomplete
journey toward full implementation

Hamilton, Cristina

Monterey, California: Naval Postgraduate School

<http://hdl.handle.net/10945/41386>

Downloaded from NPS Archive: Calhoun



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**REAL ID AND THE SECURITY OF STATE IDENTITY
DOCUMENTS: THE LONG, ROCKY, AND INCOMPLETE
JOURNEY TOWARD FULL IMPLEMENTATION**

by

Cristina Hamilton

March 2014

Thesis Advisor:
Second Reader:

Kathleen Kiernan
Christopher Bellavita

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 2014	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE REAL ID AND THE SECURITY OF STATE IDENTITY DOCUMENTS: THE LONG, ROCKY, AND INCOMPLETE JOURNEY TOWARD FULL IMPLEMENTATION			5. FUNDING NUMBERS	
6. AUTHOR(S) Cristina Hamilton				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____ N/A ____.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The 9/11 Commission recommended that the federal government set standards for the issuance of identification documents. Insecure identification documents are used to engage in fraud against individuals, government institutions, and businesses, and they have been used to facilitate terrorism. The federal government has led by enacting the REAL ID Act in 2005, which set issuance standards for driver's licenses and state identification documents. Nine years later, only 21 of the 56 states and territories are in full compliance. This thesis provides a high-level overview and evaluation of some of the major state concerns that have led some jurisdiction to resist REAL ID openly, and others to make material, but not yet full compliance. It explores the federal government's response to those concerns; how it has sought to facilitate compliance, and its more recent move toward enforcement as it begins to restrict the use of non-compliant documents for federal official purposes. The thesis provides case studies of three states to illustrate the implementation experience of those states. Finally, it provides an analysis of federal efforts to date, and provides recommendations on what the federal government might do to address states' concerns, and reach the goal of full compliance.				
14. SUBJECT TERMS REAL ID, Driver's Licenses, Identification Documents, Secure Documents, Document Fraud, Identity Theft, National ID			15. NUMBER OF PAGES 231	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**REAL ID AND THE SECURITY OF STATE IDENTITY DOCUMENTS:
THE LONG, ROCKY, AND INCOMPLETE JOURNEY TOWARD FULL
IMPLEMENTATION**

Cristina Hamilton

Division Chief, National Security and Benefits Integrity Division,
Office of Policy and Strategy, U.S. Citizenship and Immigration Services,
Department of Homeland Security, Washington, DC
B.A., University of Akron, 1983
J.D., University of Akron School of Law, 1986

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2014**

Author: Cristina Hamilton

Approved by: Kathleen Kiernan
Thesis Advisor

Christopher Bellavita
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The 9/11 Commission recommended that the federal government set standards for the issuance of identification documents. Insecure identification documents are used to engage in fraud against individuals, government institutions, and businesses, and they have been used to facilitate terrorism. The federal government has led by enacting the REAL ID Act in 2005, which set issuance standards for driver's licenses and state identification documents. Nine years later, only 21 of the 56 states and territories are in full compliance. This thesis provides a high-level overview and evaluation of some of the major state concerns that have led some jurisdiction to resist REAL ID openly, and others to make material, but not yet full compliance. It explores the federal government's response to those concerns; how it has sought to facilitate compliance, and its more recent move toward enforcement as it begins to restrict the use of non-compliant documents for federal official purposes. The thesis provides case studies of three states to illustrate the implementation experience of those states. Finally, it provides an analysis of federal efforts to date, and provides recommendations on what the federal government might do to address states' concerns, and reach the goal of full compliance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	RESEARCH QUESTION	1
B.	PROBLEM STATEMENT	2
C.	LITERATURE REVIEW	4
D.	ARGUMENTS AND CLAIMS BY PROPONENTS AND OPPONENTS	5
1.	The Secure Identity/Law and Order Camp.....	6
2.	The Libertarian/Privacy/States' Rights Camp	8
3.	The Researchers/Evaluators Camp.....	10
E.	METHODOLOGY/RESEARCH DESIGN.....	12
F.	LIMITS OF THE RESEARCH.....	14
II.	REAL ID AS A SOLUTION TO THE PROBLEM OF INSECURE IDENTITY DOCUMENTS.....	17
A.	THE REAL ID DOCUMENT SECURITY ELEMENTS.....	20
B.	DOCUMENT SECURITY AND PREVIOUS LEGISLATIVE EFFORTS, DOCUMENT SECURITY PROVISIONS OF IIRIRA	22
C.	DOCUMENT SECURITY PROVISIONS OF ITRPA	24
1.	Status of IRTPA Document Security Provisions.....	27
D.	CONCLUSION	28
III.	DOES REAL ID CREATE A NATIONAL ID?	31
A.	WHAT CONSTITUTES A NATIONAL ID?	32
1.	United States-REAL ID.....	33
2.	Understandable Concerns Are Raised by a National ID.....	37
B.	NATIONAL ID EFFORTS IN COMPARISON COUNTRIES	38
1.	The United Kingdom	39
2.	India	42
3.	South Africa.....	46
4.	Germany	50
C.	CHAPTER RECOMMENDATIONS AND CONCLUSIONS: IMPLICATIONS FOR THE IMPLEMENTATION OF REAL ID	52
D.	CONCLUSION	55
IV.	PRIVACY ISSUES ASSOCIATED WITH REAL ID	57
A.	THE 2D BARCODE	58
B.	THE RULEMAKING PROCESS AND CONSIDERATION OF RFID AS A POSSIBLE ALTERNATIVE TECHNOLOGY	60
C.	PROTECTION OF PII IN THE MRZ	62
D.	THE RFID AS AN ALTERNATIVE TECHNOLOGY	66
E.	ADDITIONAL PRIVACY PROTECTION MEASURES ADOPTED BY DHS.....	68
F.	CONCLUSION	68

V.	THE CLAIM THAT REAL ID VIOLATES THE TENTH AMENDMENT AND CONSTITUTES AN UNFUNDED MANDATE.....	69
A.	THE UNFUNDED MANDATES REFORM ACT.....	72
B.	APPLICABILITY OF UMRA.....	74
C.	CONCLUSION	77
VI.	TOOLS AVAILABLE TO ASSIST WITH IMPLEMENTATION.....	79
A.	DHS’ SUPPORT FOR VERIFICATION PROGRAMS.....	79
B.	AN OVERVIEW OF THE VERIFICATION SYSTEMS	81
C.	INCREASING PROGRESS TOWARD AN EFFECTIVE AND SECURE VERIFICATION SYSTEM.....	82
D.	CHAPTER CONCLUSION.....	87
VII.	FUNDING ASSISTANCE AND FLEXIBILITY ON DEADLINES FOR THE STATES	89
A.	EXTENSIONS OF COMPLIANCE DATES AND A MOVE TOWARD ENFORCEMENT.....	89
1.	A Series of Extensions.....	89
2.	Enforcement Comes at Last?	92
B.	CHAPTER CONCLUSION.....	96
VIII.	FINANCIAL SUPPORT PROVIDED BY DHS TO THE STATES	97
A.	DHS HAS PROVIDED SUBSTANTIAL SUPPORT TO ENCOURAGE COMPLIANCE BUT THE TRUE COSTS OF REAL ID IMPLEMENTATION ARE UNKNOWN.....	97
B.	GRANTS AND OTHER FORMS OF STATE ASSISTANCE.....	100
C.	SOME BELIEVE IMPLEMENTATION COSTS MAY HAVE BEEN LOWER THAN ESTIMATED.....	102
D.	CHAPTER CONCLUSION.....	104
IX.	THE REACTION OF THE STATES TO REAL ID.....	107
A.	SOME STATES REBELLED.....	107
B.	SOME STATES COMPLIED	110
C.	SOME STATES SOUGHT ALTERNATIVES TO REAL ID	111
D.	CHAPTER CONCLUSION.....	111
X.	DOCUMENT FRAUD AND IDENTITY THEFT.....	113
A.	THE SCOPE OF THE IDENTITY THEFT PROBLEM IN THE UNITED STATES.....	114
B.	FEDERAL RECOGNITION OF AND EFFORTS TO ADDRESS DOCUMENT FRAUD AND IDENTITY THEFT	119
C.	CHAPTER CONCLUSION.....	123
XI.	STATE CASE STUDIES.....	125
A.	DELAWARE.....	125
1.	Early REAL ID Efforts by Delaware.....	125
2.	Best Practices/Efforts by Delaware to Nudge Public Compliance	126
3.	Leadership Matters: DMV Chief, Jennifer Cohan.....	128

4.	Delaware’s Efforts and Leadership Have Been Recognized	130
5.	Media Coverage in Delaware	131
6.	Delaware Has Unique Advantages Aiding Its Implementation Efforts	132
B.	NEW JERSEY	133
1.	New Jersey’s Attempt to Implement REAL ID	133
2.	The ACLU Lawsuit	135
3.	Basis of the Lawsuit and New Jersey’s Next Steps	136
4.	New Jersey’s 6 Point ID System	137
5.	New Jersey’s Anti-Fraud Efforts	139
6.	The Enhanced Digital Driver’s License	140
7.	New Jersey’s Use of Facial Recognition Technology	141
8.	New Jersey’s Anti-Fraud Prosecutions	142
9.	New Jersey’s Media Coverage	144
C.	MAINE	145
1.	Maine’s Shifting Approach on Document Security	145
2.	The Political Backdrop Behind Maine’s Positions on REAL ID	147
3.	Once Again--Leadership Matters: Secretary of State Matthew Dunlap	147
4.	Security Vulnerabilities Exposed—Leading to a Gradual Shift	149
5.	Maine Tightens Its Driver License Issuance Process	150
6.	Emerging Divisions Among Maine Democrats	152
7.	The Pendulum Swings Back: The Fight to Roll Back REAL ID Compliance Measures	153
8.	Maine’s Privacy Related Concerns About REAL ID	157
XII.	ANALYSIS AND FINDINGS	159
A.	REAL ID IS A NECESSARY AND APPROPRIATE TOOL TO ADDRESS THE PROBLEM OF INSECURE IDENTITIES	159
B.	DHS HAS WORKED TO ADDRESS THE RANGE OF CONCERNS RAISED BY CRITICS REGARDING THE LEGISLATION AND ITS IMPLEMENTATION CHALLENGES, BUT MUST DO MORE	160
C.	REAL ID IS NOT A NATIONAL ID BUT CAUTION IS WARRANTED	161
D.	REAL ID DOES NOT VIOLATE TENTH AMENDMENT PRINCIPLES OR CONSTITUTE AN UNFUNDED MANDATE, BUT FUNDING IS A KEY ISSUE FOR THE STATES	162
E.	PRIVACY AND SAFEGUARDING OF PRIVATE INFORMATION ARE IMPORTANT CONSIDERATIONS AND ARE BEING ADDRESSED	162
F.	CONCLUSIONS	163
XIII.	RECOMMENDATIONS	165
A.	ENGAGE WITH THE GENERAL PUBLIC TO EDUCATE THEM ON THE IMPORTANCE OF DOCUMENT SECURITY EFFORTS	165
B.	PARTNER WITH STATES THAT ARE IN FULL COMPLIANCE WITH REAL ID AND/OR ARE STRIVING TO BE IN	

	COMPLIANCE AND RECRUIT STATE LEADERS THAT SUPPORT REAL ID AS NATIONAL SPOKESPERSONS	165
C.	DHS SHOULD DISPEL MYTHS ASSOCIATED WITH REAL ID AND ACTIVELY RESPOND TO CRITICS	166
D.	UNDERTAKE ANNUAL REPORTING ON STATE PROGRESS ON REAL ID AND OUTCOMES WITHIN INDIVIDUAL STATES	166
E.	USE ENFORCEMENT AS AN OPPORTUNITY TO PERSUADE AND BUILD ALLIANCES AND AVOID DEEPENING DIVISIONS, WHILE PREPARING FOR LITIGATION.....	167
F.	COMMIT TO REAL ID, AND SHOW THAT COMMITMENT THROUGH ACTIVE ASSISTANCE AND FUNDING.....	168
G.	IMPLEMENTATION OF RECOMMENDATIONS.....	168
APPENDIX A.	IDENTIFICATION DOCUMENTS HELD BY THE 9/11 HIJACKERS	173
APPENDIX B.	EVVE IMPLEMENTATION AS OF JUNE 2012.....	175
APPENDIX C.	REAL ID IMPLEMENTATION TIMELINE AS PUBLISHED IN MARCH 2008 REGULATORY EVALUATION FINAL RULEMAKING	177
APPENDIX D.	DHS’ 18 MATERIAL COMPLIANCE BENCHMARKS DEPARTMENT OF HOMELAND SECURITY	179
APPENDIX E.	THE EXTENDED TABLE OF CONTENTS FROM THE REGULATORY ASSESSMENT OF COSTS AND BENEFITS THAT ACCOMPANIED THE REAL ID FINAL RULE.....	181
APPENDIX F.	NOTICE ON REAL-ID FUNDING AVAILABILITY MADE BY FEMA.....	185
APPENDIX G.	CENTER FOR IMMIGRATION STUDIES GRANT ALLOCATION BY JURISDICTION	187
APPENDIX H.	STATE LAWS OPPOSING REAL ID	191
	LIST OF REFERENCES.....	193
	INITIAL DISTRIBUTION LIST	207

LIST OF FIGURES

Figure 1.	PDF 417 2D Stacked Barcode	58
Figure 2.	Infrastructure Solution of Electronic Data Validation and Verification	82
Figure 3.	States with SAVE Memoranda of Agreement	83
Figure 4.	Verification of Social Security Numbers	84
Figure 5.	EVVE Implementation—December 2013	86
Figure 6.	Initial Waiver and Extension for Compliance to December 31, 2009	91
Figure 7.	Enforcement Phases and Dates	93
Figure 8.	Non-compliant and Compliant/Extension States	95
Figure 9.	Number of Grants Awarded, FY2008–FY2011	101
Figure 10.	Anti-REAL ID Legislation As Enacted in States	108
Figure 11.	Image and Logo of a Delaware’s Driver’s License	126
Figure 12.	New JerseyTRU-ID Information and Image of Driver’s License	134
Figure 13.	New Jersey’s 6 Point ID System.....	138
Figure 14.	Sample of a Maine Driver’s License	154

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAMVA	American Association of Motor Vehicle Administrators
AFIS	Automated Fingerprint Identification System
AIM	Association for Automatic Identification and Mobility
ANSI	American National Standards Institute
BMV	Bureau of Motor Vehicles
CHDS	Center for Homeland Defense and Security
CIDR	central ID repository
CRS	Congressional Research Service
CSDL	Coalition for Secure Driver's Licenses
DHS	Department of Homeland Security
DLA	driver license agencies
DMV	Department of Motor Vehicles
DOS	Department of State
DOT	Department of Transportation
EDDL	enhanced digital driver license
EDL	enhanced driver's license
EPIC	Electronic Privacy Information Center
EU	European Union
EVVE	Electronic Verification of Vital Events
FEMA	Emergency Management Agency
FY	fiscal year
GAO	Government Accountability Office
GoM	Group of Ministers
HANIS	Home Affairs National Identification System
HSI	Homeland Security Investigations
ICAO	International Civil Aviation Organization
ICE	Immigration and Customs Enforcement
IGR	Intergovernmental relations
IIRIRA	Illegal Immigration Reform and Immigrant Responsibility Act of 1996
IRS	Internal Revenue Service
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ITIN	individual taxpayer identification number
ITS	Identity Theft Supplement

LGBT	lesbian, gay, bisexual, and transgender
MCLU	Maine Civil Liberties Union
MNIC	multipurpose national identity card
MOA	memorandum of agreement
MOU	memorandum of understanding
MRZ	machine-readable zone
MVC	Motor Vehicle Commission
NAC	Nebraska Avenue Complex
NAPHSIS	National Association of Public Health Statistics and Information Systems
NCSL	National Conference of State Legislatures
NCVS	National Crime Victimization Survey
NGA	National Governors Association
NPR	Notice of Proposed Rulemaking
NSA	National Security Agency
NYCLU	New York American Civil Liberties Union
OIG	Office of the Inspector General
OPRA	Open Public Records Act
PDF	portable data file
PDF417	Portable Data File 417 barcode
PIA	privacy impact assessment
PII	personally identifiable information
RFID	radio frequency identification
SAVE	Systematic Alien Verification for Entitlements
SSN	Social Security number
SSOLV	Social Security Online Verification
TIGTA	Treasury Department's Inspector General for Tax Administration
U.S.	United States
UIDAI	Unique Identification Authority of India
UK	United Kingdom
UMRA	Unfunded Mandates Reform Act of 1995
USCIS	U.S. Citizenship and Immigration Services
VRA	vital records agency
WHITI	Western Hemisphere Travel Initiative

EXECUTIVE SUMMARY

The attacks of 9/11 served as a wake-up call that the United States (U.S.) was vulnerable to terrorism on U.S. soil and that it was unprepared to address that threat. The 9/11 Commission undertook a thorough examination of how it happened that the nation was unprepared and what needed to be done to avoid such a tragedy in the future. It issued a limited set of recommendations that it believed to be the most important, and whose implementation could make the greatest difference, as stated in the Preface to the 9/11 Commission Report. One of those recommendations addressed the vulnerability posed by insecure birth certificates and identification documents, which enabled the hijackers to remain in the United States and board the planes. Noting that secure identification should begin in the United States, it recommended that the federal government establish standards for the issuance of such documents. That recommendation led to the enactment of the REAL ID Act of 2005. The law was, and remains controversial, and its implementation through the state driver's license and ID issuance process has proven contentious, difficult, and slow. Nearly nine years after the enactment of REAL ID, only 21 states and territories are in full compliance with the law's requirements and another 35 range from being in or working toward material compliance, or remain in a status of non-compliance—some defiantly so. The current state of affairs falls short of fulfilling the objectives behind the 9/11 Commission's recommendation. This author sought to understand why implementation of the law has proven so difficult, why full implementation is desirable, and what the Department of Homeland Security (DHS) has done and can do to assist states seeking to achieve full compliance. What the author discovered is that REAL ID and the problems that it seeks to address are complex, and multi-faceted. The issues posed by insecure identity documents and the proposed remedy represent a complex homeland security policy and implementation issue with significant real life impacts upon individuals, government entities, and institutions, which requires much attention, effort, and informed discourse. The existing literature consists of a myriad of background documents, advocacy pieces, and assessments of REAL ID by a variety of different individuals and entities. This thesis is intended as a resource that can

serve as a starting point for those who seek a general overview and background on the primary issues surrounding REAL ID, where things stand in regard to state implementation, and some possible ways forward.

THE THESIS OBJECTIVES AND THE APPROACH

The objective of this thesis is to examine, through an evaluative and case study approach, the principal issues that have contributed to the slow adoption of, and in some instances, the active defiance of the law; how DHS has responded to and sought to address those issues; and what more can be done to promote full implementation. This thesis offers three things to readers: 1) an overview of REAL ID requirements, and a high-level examination of the major issues of concern to the states and critics related to those requirements, 2) an examination of case studies of three states arrayed along the continuum of implementation milestones, ranging from being in full compliance, in material compliance, and in non-compliance, and 3) an analysis of the factors that have led to the current implementation status, and recommendations for how DHS should proceed as it seeks to achieve compliance by the states and territories.

THE ANALYSIS AND FINDINGS

REAL ID has attracted both proponents and opponents of the law, and it has created unlikely alliances, often between liberal entities and those promoting libertarian principles that emphasize freedom from government regulation and requirements. On the other side, are individuals and entities concerned about the risks of terrorism and criminality associated with insecure identity documents, and who favor decisive action by the federal government to enhance national and individual security. A place also exists for more neutral entities, or evaluators, generally from academia and government entities, such as the General Accountability Office, and the Congressional Research Service. The fact that the law engenders such a broad range of interests and generates strong views is reflective of the difficulty of gaining consensus on the various issues raised by the law. Opponents have raised several concerns with the legislation. The principal ones are whether the legislation creates a national identification system, whether it poses an

infringement on state sovereignty, whether it constitutes an unfunded mandate, and whether it poses a risk to individual privacy and security of information.

The federal government, largely through DHS, has sought to rebut or mitigate these concerns through the rulemaking process and the associated privacy impact assessments, as well as assistance and grants. It has provided an array of tools to assist states in verifying the information submitted in support of the applications, and it has provided funding directly to the states in support of efforts to build up the verification capabilities and providing tools, such as the Systematic Alien Verification for Entitlements (SAVE) system, designed to verify the immigration status of individuals, and the Electronic Verification of Vital Events (EVVE) system, designed to verify vital records information. The individual state grants are designed to help states make the necessary modifications to their issuance systems.

DHS has also postponed the consequences that would fall to individuals holding non-REAL ID compliant documents. Those consequences prohibit the acceptance of such documents for federal official purposes, such as entry into federal buildings, and the most significant effect, the non-acceptance of such documents for purposes of boarding commercial aircraft. It has created the concept of material compliance, which rewards states moving toward compliance by allowing their documents to continue to be used for federal purposes, principally to board commercially regulated aircraft. Yet, it has also determined that it will begin to enforce the requirements.

State reaction has been mixed and has ranged from states that sought to be in full compliance early in the process, to states that have taken important, but not complete steps toward full compliance, and states that have openly defied REAL ID, and in some cases, have passed laws restricting their ability to comply. The thesis discusses the experience of three East Coast states, Delaware, New Jersey, and Maine, to illustrate the range of states responses and implementation challenges.

The thesis also sought to explore additional consequences arising from insecure identification documents beyond terrorism, emphasized by the 9/11 Commission in its report. In that regard, the thesis explores the role of insecure identification documents in

identity fraud and identity theft, a consequence that has had profound effects on individuals and government and financial institutions. This issue was addressed, as it is important for these additional effects of insecure identity documents to be factored in the ongoing implementation effort surrounding REAL ID, particularly as the stark memory of 9/11 recedes, and the consequences of fraud and identity theft continue to increase, and themselves pose national security risks beyond the consequences to the individual, governmental and financial systems.

This paper undertakes a broad examination of REAL ID, as well as an analysis from which the following findings have emerged.

- REAL ID is a necessary and appropriate tool to address the problem of insecure identities
- DHS has worked to address the range of concerns raised by critics regarding the legislation and its implementation challenges, but must do more
- REAL ID is not a national ID but caution is warranted
- REAL ID does not violate Tenth Amendment principles or constitute an unfunded mandate, but funding is a key issue for the states
- Privacy and safeguarding of private information are important considerations and are being addressed

As DHS continues to work to have states achieve full compliance, some lessons and recommendations can guide DHS' future efforts.

- Engage with members of the general public to educate them on the importance of document security efforts
- Partner with states that are in full compliance with REAL ID and/or are striving to be in compliance and recruit state leaders who support REAL ID as national spokespersons
- DHS should dispel myths associated with REAL ID and actively respond to critics
- Undertake annual reporting on state progress on Real ID and outcomes within individual states
- Use enforcement as an opportunity to persuade and build alliances and avoid deepening divisions, while preparing for litigation
- Commit to REAL ID, and show that commitment through active assistance and funding

CONCLUSION

The federal government has sought to implement the 9/11 Commission's recommendation and has set federal standards for the issuance of driver's licenses and state identification documents. The task of achieving full implementation of REAL ID through the adoption of those standards by the 56 states and territories has proven to be more challenging, and the timeframe more lengthy than many may have anticipated. The complex policy and implementation issues arising from REAL ID are important, difficult, and DHS must continue to address them with careful consideration and meaningful action. REAL ID can be seen as promoting the security of society, and protecting individuals, as well as government and private institutions, from a range of negative stemming from insecure documents. These range from more simple forms of identity theft leading to inconvenience, to more serious forms of fraud and identity theft resulting in significant financial impacts on individuals and institutions, and ultimately, the most serious consequence—terrorism. The challenge that remains is to achieve full compliance so that weak links in the nation's identity issuance system do not compromise the whole system and contribute to an insecure document issuance system. The journey has been long and the final destination on the road to full compliance with REAL ID has not been reached—but the destination is within sight.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Participating in this program has been one of the great privileges in my life. It has pushed me to think more carefully about the issues I have dealt with every day of my career, and exposed me to many things that I had not thought about—but should have. It has given me the luxury of thinking critically about homeland security and its future more than I have ever had the opportunity to do. It has also exposed me to great homeland security educators and practitioners who have imparted their knowledge and experience to us all. I will always be grateful to U.S. Citizenship and Immigration Services (USCIS) for allowing me to have this opportunity. My thanks to all of the people at the Center for Homeland Defense and Security (CHDS) involved in making this program what it is today, and who strive to make it even better. Special thanks to my committee, Dr. Kathleen Kiernan, for her encouragement and belief in me, and to Dr. Chris Bellavita, who often knows me better than I know myself, whose dedication to this program is so apparent, and without whom, the program would not be what it is today.

For me, the most valuable aspect of this program is the privilege I have had to work with and learn from my fellow cohort members. A finer group of dedicated professionals could not have come together to make this experience as valuable for me as it has been. I have learned from all of you and consider you my friends, as well as my fellow students. I wish to particularly thank my NCLB group, my “DC Cohort” regulars, and especially Captain Tim Wendt, whose constant help, limitless patience, and valued friendship has helped me immeasurably throughout this program.

I knew when I began this journey that it would be a lot of work for me, but what I did not fully appreciate was how much work it would be for my husband, Bob. I could not have asked for a more supportive spouse as I have traveled this difficult, but rewarding journey. You have been selfless and have taken on so much so that I could succeed and keep my sanity. For that, I thank you and love you.

I thank the rest of my family for their love and support, and dedicate this effort to my father and to the memory of my paternal grandmother. They instilled in me the value of education, the need to constantly improve, and the determination to succeed. I also wish to recognize my sons, Mark and David, who represent the future and why homeland security is such a critical issue for me. I am most proud of being your mother.

I. INTRODUCTION

Insecurity about the true identity of those with whom we interact, and concerns about the type of fraud and systemic vulnerabilities that facilitated the ability of the 9/11 hijackers to remain in the United States and travel, have forced American society to grapple with the issue of the security of identity documents and the consequences that would flow from requirements to enhance the security of the identity document issuance system.

This thesis explains that current discussion, and describes the threats that an insecure identity document issuance system poses to national security, to the identity security of individuals, and the security of commercial and other transactions in U.S. society. It also examines the thorny and complex policy and implementation issues surrounding the REAL ID Act (REAL ID).¹ Finally, it examines the progress made to date under the current legislation, examines the implementation efforts of sample states as case studies, and looks at efforts of the federal government to facilitate full compliance.

A. RESEARCH QUESTION

This thesis seeks to answer the following: whether, despite protestations by the states, the REAL ID Act is a necessary and effective solution to the problem of insecure driver's licenses and identity documents and whether it does so in a way that addresses concerns, such as privacy issues and concerns about a de facto national ID system, whether its existence has had the salutary effect of dragging the states, slowly but surely, toward more secure documents, and possible full compliance with the Act, and whether implementing REAL ID shows promise as an effective mechanism to help address the problem of identity theft. This paper explores the progress of state implementation efforts and identifies factors that have contributed to the success of the states that have been found by the Department of Homeland Security (DHS) to be in compliance with the

¹ *The REAL ID Act of 2005*, Public Law 109–13, Div. B, 119 Stat. 231, 302, 2005, REAL ID Public Law.pdf.

legislation, as compared to states not in compliance, and some effects of REAL ID within the compliant states. Finally, it also examines efforts by DHS and the federal government to promote compliance, and makes recommendations as to what more the federal government should do to have the states achieve full implementation.

B. PROBLEM STATEMENT

This country's ability to verify the true identity of persons is critical to the protection of the nation and its people from a variety of threats to national, individual, and economic security. The terrorist attacks inflicted upon the United States on 9/11 dramatically illustrated this problem when it was determined that all or nearly all of the hijackers had obtained identity documents in the form of driver's licenses and identity documents, to embed themselves in the United States; six of the hijackers used the state issued identity documents as proof of identity in boarding the aircraft, and three of those documents were fraudulent. The national security nexus is only one aspect of the problem posed by insecure identity documents; it also includes the growing problem of identity theft, and fraud perpetrated upon government, financial institutions, and business entities.

The events of 9/11 provided an opening and an imperative for the federal government to set standards for the issuance of state driver's licenses and identification documents. Prior to that time, standards for such documents were set by the states, and were governed by no national standards.² Following the attacks, and consistent with recommendations of the 9/11 Commission, Congress passed the REAL ID Act, in May 2005, which set federal standards for the issuance of state identity documents, to include driver's licenses and state identification cards. Addressing insecure documents poses significant policy issues. Among them are the proper balance between the power of the federal government and the authority reserved to the states, and concerns about establishing an actual or de facto national identity document. This paper examines the various criticisms of the REAL ID, as well as its benefits and contributes to the issue by consolidating the literature and addressing how the implementation efforts have

² Michael J. Garcia, Margaret M. Lee, and Todd Tatelman, *Immigration: Analysis of the Major Provisions of the REAL ID Act of 2005* (Washington, DC: Congressional Research Service, May 25, 2005), 38, <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA453701>.

negatively or positively impacted individual and societal considerations associated with identity security, as well as exploring key policy issues and implementation challenges.

Nearly nine years have elapsed since the enactment of REAL ID and state implementation efforts have been uneven and inconsistent, ranging from full compliance, steady progress toward compliance, to active defiance. On December 20, 2013, DHS announced that it had certified 21 states as being in full compliance with REAL ID; in other words, those states had met the minimum standards under the legislation for improving the security of state issued driver's licenses and identification cards.³ DHS further indicated that it had granted extensions to another 20 states and territories that had submitted information indicating that they were on the pathway to full implementation.⁴ Through its announcement, DHS also stated that beginning in 2014, it would begin "an achievable schedule" for the "phased enforcement" of REAL ID.⁵ News reports at the time indicated that two states, Arizona and Pennsylvania, had failed to submit status reports on their compliance efforts.⁶

This paper also begins to address the knowledge gap that exists relative to the implementation efforts of the states and the issues, impediments, and in some cases, successes they have had. It accomplishes this task through illustrative case studies of three states, including a state that has achieved full compliance with REAL ID (Delaware), in contrast to a state that has actively resisted compliance with the law, (Maine), and a state that had made efforts to achieve compliance but whose efforts to comply were thwarted by litigation designed to prevent compliance with the law (New Jersey).

The paper explores the potential benefits of REAL ID beyond the federal purposes specified in the legislation, specifically, benefits in addressing problems, such as identity theft. It also discusses some of the efforts that have been made by the federal

³ "DHS Releases Phased Enforcement Schedule for REAL ID," accessed December 29, 2013, <http://www.dhs.gov/news/2013/12/20/dhs-releases-phased-enforcement-schedule-real-id>.

⁴ Ibid.

⁵ Ibid.

⁶ Reuters, "REAL ID Enforcement Begins in 2014, 21 States Compliant," December 20, 2013, <http://www.reuters.com/article/2013/12/20/csdl-dhs-real-id-act-idUSnPnDCfLrqh+168+PRN20131220>.

government to assist the states in achieving compliance through grants awarded, the availability of tools to facilitate verification of the documents and information used to obtain licenses and identification documents. It discusses recent efforts by the federal government to enforce compliance deadlines. Finally, the paper recommends additional measures that DHS can take to encourage compliance.

This effort is worthy of graduate level research because the issues that REAL ID seeks to address are multi-faceted, the remedy is controversial and expensive, seen by many as unproven, and is alleged to impact individual and states' rights adversely. In short, the problem of insecure documents, and REAL ID as the identified solution, represents a complex homeland security policy and implementation issue with significant real life impacts upon individuals, government entities, and institutions, which necessitates much attention, effort, and informed discourse.

C. LITERATURE REVIEW

In the aftermath of 9/11, the United States sought to address vulnerabilities in its issuance of state driver's licenses and identity documents to ensure that such documents were not used to enable terrorists to embed themselves in the United States using false identities. The United States did so by enacting legislation known as the REAL ID Act of 2005 (REAL ID), which required the federal government to set standards for the issuance of driver's licenses and state issued identification documents.⁷

This literature review explores the treatment of some of those issues, by focusing on views reflecting the competing camps that examine the balance between security versus privacy and civil liberties, the federalism issues implicated by federal action versus states' rights, and the question about whether REAL ID establishes a national ID. It begins to explore literature on the technology utilized, the interoperability requirements, and how the discussions regarding the risks to privacy are being affected. Also touched upon in this thesis, and being further explored, is literature on the implementation challenges being faced by the states to include what obstacles they face

⁷ *The REAL ID Act of 2005.*

in terms of compliance, and how, at the state level, they are addressing or not addressing the privacy concerns raised by REAL ID.

D. ARGUMENTS AND CLAIMS BY PROPONENTS AND OPPONENTS

A number of proponents and opponents have spoken or written about the policy and legal issues posed by REAL ID. These concerns are reflected in the literature that has surrounded the enactment of the law and the subsequent efforts to modify its provisions, as well as efforts to repeal it and pass alternative legislation. The discussion in public forums, such as the news, in Congress, in think tank discussions, and the debate emanating from written commentary and scholarly writings, breaks down principally into two divergent philosophies on the issue of identity and document management, and one more neutral position taken by some commentators. On one side are those who favor a stronger role of government through standards and such in the management of identity related documents, such as driver's licenses and identity cards. This paper refers to this group as the secure identity/law and order camp. The reasons these individuals and groups offer in support of REAL ID generally fall into the areas of: 1) enhancing security generally, including more specifically preventing terrorism, 2) favoring REAL ID as a way to address the problem of identity theft due to its effects on individuals and society, and 3) favoring REAL ID as a means to hamper other forms of criminality and adverse effects on society, such as those stemming from the use of false identity documents, underage drinking, or the avoidance of legal obligations like child support or unauthorized employment.⁸

On the other side are those opposed to such government efforts due to concerns about a government that encroaches on people's individual rights, puts privacy at risk, and violates states' rights by having government impose standards in violation of 10th Amendment principles, and does so in a way that creates unfunded mandates on the states. The camp opposed to REAL ID has posed several arguments against the legislation and its implementation. Principal among them is that REAL ID is a national

⁸ Janice Kephart, "Repealing REAL ID? Rolling Back Driver's License Security," *Backgrounders*, Center for Immigration Studies, June 2009.

ID by another name.⁹ Other concerns relate to the presumed illegality of such a program, its privacy implications, concern about governmental abuses of power, and the costs of implementing the law's requirements. This paper refers to this group as the libertarian/privacy/states' rights camp.

In between the two, or at least not explicitly taking sides, is a more neutral group that neither explicitly supports nor opposes REAL ID, but instead employs a more rigorous, evaluative mode offering assessments and recommendations. This paper refers to this group as the researchers/evaluators.

1. The Secure Identity/Law and Order Camp

The principal representative of this camp is Janice Kephart, currently, a National Security Fellow, and formerly, the Director of National Security Policy at the Center for Immigration Studies, a Washington, DC think tank that focuses on immigration issues.¹⁰ Ms. Kephart has published numerous articles on this issue, none of which focus exclusively or even primarily on the immigration implications of REAL ID as her current affiliation might suggest.¹¹ The law and order/secure identity camp approach the issue from two principal positions. One is that non-secure state identification documents are vulnerable to misuse by individuals posing a national security threat to the United States, and why it is imperative that REAL ID be implemented to reduce the risk of terrorists

⁹ Electronic Privacy Information Center, *REAL ID Implementation Review: Few Benefits, Staggering Costs: Analysis of the Department of Homeland Security's National ID Program*, May 2008, 3. [Hereinafter EPIC: *Real ID Implementation Review*]. See also Daniel J. Steinbock, "Fourth Amendment Limits on National Identity Cards," in *Privacy and Technologies of Identity: A Cross-disciplinary Conversation*, ed. Katherine Jo Strandburg and Daniela Stan Raicu, CIPLIT Symposium on Privacy and Identity: The Promise and Perils of a Technological Age (New York: Springer Science+Business Media, 2006). (Steinbock cites in footnote 1 to various articles from the last 20 years in which conversations regarding national IDs are referenced.)

¹⁰ Ms. Kephart is a particularly prolific writer in support of REAL ID and brings to the issue her past perspective as counsel to the 9/11 Commission.

¹¹ Kephart has authored at least five articles on behalf of the Center for Immigration Studies related to REAL ID: Janice Kephart, "REAL ID Final Rules: A Summary," *Center for Immigration Studies*, March 2008; Janice Kephart, "The Appearance of Security, REAL ID Final Regulations vs. Pass ID Act of 2009," *Backgrounders*, *Center for Immigration Studies*, April 2009; Kephart, "Repealing REAL ID? Rolling Back Driver's License Security"; Janice Kephart, "REAL ID Implementation: Less Expensive, Doable, and Helpful in Reducing Fraud," *Center for Immigration Studies*, January 2011, <http://cis.org/real-id>.

using identity documents to embed themselves in society and go unnoticed.¹² The second general theme is that identity documents must be made secure to reduce the ever-growing threat of identity theft given the implications that it has for individuals and the security of commercial and governmental transactions. This camp sees strengthening the security of identity documents as a win-win for society and for the individual. As noted by one member, “[c]reating a secure identity document is needed to help keep America safe, free, and prosperous.”¹³ Members of this camp dispute the notion that the REAL ID provisions establish a national ID by noting that implementing the law does not require any aggregation of data into a centralized database operated by the federal government.¹⁴ It should be noted that allied members of this camp also include outspoken advocates of a national ID system. However, the reasons they support such a system are similar to those that see direct and indirect benefits of greater security in identity documents that further, in their view, national security and the prevention of terrorism.¹⁵

Finally, the federal government, under the administration of President George W. Bush, should also be considered a member of the secure identity/law and order camp. While no longer in office, and largely silent in the current debate, its engagement on the issue indicates agreement with the general positions of this camp. It rejected the idea that REAL ID was creating a de facto national ID system, noting in its privacy impact assessment (PIA) issued in conjunction with the final rule, the preamble to the rule stated, “DHS does not intend that a REAL ID document become a de facto national ID based on the actions of others outside of DHS to limit their acceptance of an identity document to a REAL ID-compliant driver’s license or identification card.”¹⁶ The PIA further noted that neither the law nor the final rule expressly create a centralized database of all drivers’

¹² Federation for Immigration Reform, “Identity and Immigration Status of 9/11 Terrorists (2011),” November 2011, <http://www.fairus.org/issue/identity-and-immigration-status-of-9-11-terrorists>.

¹³ James Jay Carafano, Ph.D., “Web Memo: DHS Gets REAL ID Right,” *The Heritage Foundation*, February 7, 2008, <http://www.heritage.org/research/reports/2008/02/dhs-gets-real-id-right>.

¹⁴ Kephart, “Repealing REAL ID? Rolling Back Driver’s License Security,” 4.

¹⁵ Alan Dershowitz, “Thinking About National ID Cards,” May 2002, <http://triton.towson.edu/~swartout/cosc311/dershowitz2.htm>.

¹⁶ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*, January 11, 2008, 6.

information.¹⁷ It should be noted that the Bush administration recognized that certain risks were inherent in implementing REAL ID. Its PIA addressed the various privacy and security concerns raised during the rulemaking process and developed a set of recommendations for the states to follow in implementing REAL ID. Known as “Best Practices for the Protection of Personally Identifiable Information Associated with State Implementation of the Real ID Act,” these recommendations were included as an appendix to the PIA.¹⁸

Overall, the law and order/secure identity camp is comprised of more conservative think tanks and writers, which generally support strengthened measures to enhance national security, and have greater confidence in a system that issues identity documents at the state level through adherence to common standards, rather than through the current individual state standards approach administered as rigorously or loosely as individual states determine.

2. The Libertarian/Privacy/States’ Rights Camp

The Electronic Privacy Information Center (EPIC) issued its review of the proposed implementation of the REAL ID Act in May 2008. Its arguments are representative of those raised by those who oppose REAL ID, although EPIC can be seen as taking a “kitchen sink” approach on identifying every conceivable argument that any opponent of REAL ID might raise. The arguments fall into seven basic areas. First, that REAL ID represents an effort to establish a national ID system, despite numerous historical and more current expressions of Congress’ opposition to such a system when it established DHS. Second, REAL ID was passed with little public input, and when the rulemaking process afforded an opportunity to comment, over 21,000 public comments were received with a multitude of organizations collaborating to express their opposition to a program resisted by state governments, civil liberties advocates, and security experts. Third, it is an involuntary program imposed upon the states, and thus, an unfunded mandate. Fourth, the standards for documentation that must be submitted to the states, for

¹⁷ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*.

¹⁸ *Ibid.*, 17, attachment A.

states to verify an individual's identity prior to issuing state documents create burdens for many segments of society that may not be able to produce underlying documents, and necessary exceptions have not been provided for in the program. Fifth, problems with the regulations' data verification procedures have not been addressed, such as availability, data integrity, and the role of state DMV employees becoming enforcers of immigration laws. Sixth, the necessary privacy protections established by the federal government do not exist, which leaves this important issue to the states with numerous insider and outsider threats to the privacy of the information remaining unaddressed. Seventh, REAL ID creates new national security risks as the rules allow individuals to use a foreign passport to access the facilities to which a REAL ID would provide access.

The ACLU, arguably the most well-known entity advocating on the issue of civil rights, has provided its own assessment of REAL ID, and echoes many, if not all of the arguments raised in EPIC's assessment.¹⁹ However, the ACLU's assessment, reflected in a report by its New York affiliate, the New York Civil Liberties Union, is not as worthy of serious consideration given its alarmist, exaggerated, and at times, inaccurate, presentation of the REAL ID provisions. By way of example, it presents a hyperbolic discussion—even extending to the title, “Government Spying on Americans’ Everyday Activities,” and includes the statement, “Under a REAL ID regime, Americans will be forced to go through an endless series of electronic checkpoints in the course of their daily routines.” Later in the same document in its section entitled, “A History of Government Abuse and Data Mining,” it makes the following statement: “The REAL ID system is the next massive surveillance scheme designed to allow the government to collect large amounts of information on Americans’ lives with little oversight by Congress of the public.”²⁰

Also, writers in academic journals criticize the federal government's efforts to establish uniform standards for driver's license and identification documents. One representative journal has noted that the effort will result in a de facto national ID card,

¹⁹ New York Civil Liberties Union, *No Freedom Without Privacy: The Real ID Act's Assault on Americans' Everyday Life*, February 2009.

²⁰ *Ibid.*, 16–18.

and will facilitate a “function creep” that adversely implicates privacy, noting that doing so under national security justifications reflects either “function creep or ignorance.”²¹

3. The Researchers/Evaluators Camp

The researchers/evaluators approach the issue from the framework of legal analysis (researchers), or examination of issues related to or directly impacted by REAL ID (evaluators). The researchers in this literature review are lawyers. They understandably addressed legal considerations posed by a national ID system. A consensus appears to exist that it is likely that the REAL ID framework itself does not actually establish a national ID; yet, it may make such a phenomenon more likely.²² A central concern of the researchers is the need for dialogue on the issue of national ID cards based on their view that given the substantial and powerful advocacy in favor of national identity cards, “we will have a national debate on ID cards, if we are lucky; if we’re unlucky, we’ll dispense with the debate and go straight to the cards and the database.”²³

In terms of the legal constraints, some believe that given a recent Supreme Court precedent decision involving requests for individuals to identify themselves during a *Terry* stop, that it might be likely for the Court to uphold a requirement for individuals to present, upon request, an identification document.²⁴ The principal concern relative to the Fourth Amendment is that the decision may have changed the psychological dynamic between citizens and police, and that it may make it more likely that the country will adopt a national ID.

In general, the researchers seem less concerned about the fact that the federal government is setting standards, or even that it is running a centralized database—and

²¹ Serge Egelman and Lorri Faith Cranor, “The REAL ID Act: Fixing Identity Documents With Duct Tape,” *I/S A Journal of Law and Policy* 2, no. 1 (2006).

²² Steinbock, “Fourth Amendment Limits on National Identity Cards,” in *Privacy and Technologies of Identity: A Cross-disciplinary Conversation*. (Steinbock cites in footnote 1 to various articles from the last 20 years in which conversations regarding national IDs are referenced.

²³ A. Michael Froomkin, “The Uneasy Case for national ID Cards,” in *Securing Privacy in the Internet Age*, ed. A. Chander, L. Gelman, and M. J. Radin (Stanford: Stanford Law Books, 2008), 295–321.

²⁴ *Ibid.*, 295–296.

they acknowledge that REAL ID does not set up such a database. The researchers assert that while many people react negatively to the idea of a government-sponsored national ID system, the marginal harms of a well designed national ID system “are fewer than one might initially believe given the ways in which invasive technologies are reducing personal privacy.”²⁵

Rather, the concern is that they see that even non-centralized databases, when combined with the many private databases containing information on individuals, constitutes the equivalent of a national identity system. The researchers would prefer that the federal government exercise some type of management of such a vast system of data, and regulate its use. It is felt that building protections into such a federally managed system could serve to establish rules on the use of the data and provide more protection for the data than it would otherwise have.

There has also been a contribution to the literature on REAL ID by entities that can be described as the evaluators or auditors. These contributors, largely government or academic entities, suggest that the conversation might be influenced largely by the increasing problem of identity theft, which many assert can be curtailed through greater efforts to secure the identification document issuance process.²⁶ The problem of identity theft is growing, and affects more than 8.1 million Americans who have incurred a mean of \$631 in costs as a result.²⁷ The ties between identity theft and other types of crimes, such as credit card fraud, document fraud, and employment fraud, are recognized as having implications not just for the nation’s economy but also its security.²⁸ In addition to identity theft, one source identifies weaknesses in the individual taxpayer identification number program (ITINs), which indicates that the application process for ITINs is subject to fraud, and that state driver’s license bureaus are allowing ITINs to be used by illegal

²⁵ Froomkin, “The Uneasy Case for national ID Cards,” in *Securing Privacy in the Internet Age*, 297.

²⁶ U.S. Government Accountability Office, *Driver’s License Security: Federal Leadership Needed to Address Remaining Vulnerabilities* (2012).

²⁷ Kristin M. Finklea, *Identity Theft: Trends and Issues*, CRS Report R40599 (Washington, DC: Congressional Research Service, February 15, 2012), 1.

²⁸ Ibid.

aliens to obtain driver's licenses, even though ITINs are only to be used only as a taxpayer identification number.²⁹

E. METHODOLOGY/RESEARCH DESIGN

The research design/methodological approach is two-fold, and first encompasses an evaluative study of REAL ID and the policy issues surrounding its value and risks, and second, an examination of steps taken and obstacles encountered related to its implementation, including a focus on the experiences of three states and their approach to implementation. The evaluative portion of the thesis examines the law, provides a general overview of implementation efforts at the federal and state level, and addresses relevant legal, policy, and societal aspects to include civil liberties, federalism, and political and pragmatic concerns, such as the law's effect on document security and identity theft. The second part of the thesis discusses implementation issues generally, and illustrates those issues using a case study approach examining three different categories of states as represented by three states. The experiences of these states demonstrate distinct implementation issues and approaches. The thesis discusses how those states dealt with, and are continuing to deal with, the law's implementation and the factors contributing to each state's implementation posture.

The topic was selected because it presents challenging policy and operational issues, and reflects the tension between the desire for greater collective security by control of threats to society and to individuals, against the impacts and controversy surrounding such post 9/11 policies. It illustrates the dynamic of greater security and the resulting pragmatic concerns, such as implementation costs, the gap between the technology and the operational needs, the political dynamics surrounding the role of federal and state governments, and the allocation of roles and responsibilities between federal and state entities.

²⁹ Treasury Inspector General for Tax Administration, *Substantial Changes Are Needed to the Individual Taxpayer Identification Number Program to Detect Fraudulent Applications* (Washington, DC, July 16, 2012), <http://www.treasury.gov/tigta/auditreports/2012reports/201242081fr.html>. Another area worth exploring but which is beyond the scope of this thesis is what effect enhancing identity documents under REAL ID has had on identity theft and related fraud in those states that have implemented the provisions of the law, relative to states not yet REAL ID compliant, or that have passed legislation refusing to comply with REAL ID.

The three states selected for the case study portion of the thesis paper (Delaware, Maine, and New Jersey), were selected to illustrate a range of state approaches to the implementation of REAL ID, while focusing on a particular region of the country. The case studies discuss factors that influenced each state's approach, and the measures each took to implement, or to resist implementing, REAL ID. It also seeks to demonstrate the result of each state's efforts including some benefits and possible negative consequences. Delaware represents the states that have been most proactive on implementation, Maine would represent states adamantly opposed to implementation, and New Jersey is a state that sought implementation, yet faced a tremendous challenge, through litigation that ultimately derailed its efforts to comply but not its efforts to improve document security.

The data sources to be collected and used include the research from various sources reflected in the literature review, state and federal documents, and other available resources that reflect or comment on the interaction of the states and DHS on implementation efforts. Additional data include crime statistics, data related to identity theft, and other information regarding the misuse of identity documents in connection with crime.

The method being used is the evaluative and case study mode of analysis. Within the scope of the evaluation are specific issues such as: civil liberties; federalism; and the tools and assistance made available to states. It also examines the effect of insecure identification documents on personal, and financial security, and on the program integrity involving federal or state tax, and benefit programs.

While much has been written about REAL ID, the vast majority of the written work and analysis has focused on the events leading to the law's passage, opposition to the law, discussions of the law's requirements, and the anticipated effects of the on privacy and civil liberties of individuals. Only a few works have sought to provide updates on the implementation efforts. Fewer still have sought to provide a critical review of the issues that have contributed to slow-adoption by the states. No documents have been identified by the author that have undertaken case studies examining factors that have led certain states to be rapid adopters, and others to continue to resist adoption, and how those states have fared.

Readers of the thesis have access to a broad-based treatment of REAL ID consisting of an overview of its background, its provisions, objectives, and identified criticisms. They have a basis to understand better the complexities of efforts to secure state driver's licenses and identification cards, as well as better appreciate the reasons why it was important to undertake such an effort. They are exposed to the range of practical and political issues surrounding state efforts to implement, or not, REAL ID, and the unique implementation challenges that many states faced. More specifically, they emerge with a better understanding of the factors that led some states to implement the law successfully, while others refused or were prevented from doing so. The thesis can be read from start to finish, but its individual chapters can also serve as a brief overview for those wanting a general understanding of a variety of distinct issues associated with REAL ID, with references to literature in which a more in-depth treatment of a particular issue can be found. Two groups of intended readers that could find the thesis particularly useful include state officials in states that have not yet achieved full compliance, and DHS and federal officials charged with overseeing or evaluating implementation of REAL ID. Both groups are able to see the issues associated with REAL ID implementation, may identify ways to mitigate concerns, and see the benefits of compliance, and how it is best achieved. Finally, other readers who find it useful are individuals interested in seeing how a complex policy issue involving both state and federal elements can be navigated, and learning what actions can be undertaken to implement a complex regulatory structure designed to enhance national and individual security.

F. LIMITS OF THE RESEARCH

This thesis seeks to provide readers with a source that provides a broad overview of the variety of issues surrounding REAL ID, to demonstrate why it a complex manifestation of national security policymaking, and to demonstrate the ways it has posed implementation challenges for the federal government and the states. Through the case studies, it also seeks to give readers a sense of the differing issues confronting states, to encompass, practical, political, and social acceptance issues that have played a role in how each of the states have approached the issue of REAL ID implementation. While the

thesis seeks to consolidate and provide both a macro perspective, and with the case studies, a more micro treatment of the implementation challenges, limits to the research should be noted in this paper. First, a wealth of information is available on the various issues associated with REAL ID. This paper is already quite lengthy, and an adequate treatment of the literature would itself require a good-sized book, let alone a lengthy thesis. Second, much is not publicly available, such as the exchanges between DHS and state officials on each state's respective implementation efforts. Access to that information would be very informative, and would itself be the subject of a truly in-depth examination of the implementation challenges for the states. Although that information can occasionally be located through mechanisms like Google searches, insufficient information is publicly available that would have allowed a discussion of those exchanges in this thesis—even as to the three case study states, Delaware, New Jersey and Maine. Third, within the last year or so, an issue of particular interest to the author, and to many others, has arisen that adds an additional dimension to the discussion. That issue is the increasing debate over whether to provide illegal aliens, also referred to as undocumented aliens or undocumented immigrants, with state issued driver's licenses. It is an interesting issue in terms of the overall immigration policy debate, but also in the context of the discussion over REAL IDs implementation, and the fact that in part, REAL ID was also seen as a measure that could address illegal immigration. Most importantly, the effect of such policies on the objective of REAL ID, to issue driver's licenses and state identity documents pursuant to consistent federal standards, may be compromised or at least complicated. This is because REAL ID requires verifying the status of aliens in the country, and only issuing state identity documents to coincide with the period of authorized stay. This poses additional issues that may extend to the ability of the law to succeed and accomplish its objectives. While such state identity documents will not be REAL ID compliant, they potentially complicate, rather than streamline, the document issuance process for states and add ambiguity to the overall issue of secure identity document that serve federal, state, and institutional purposes. This topic itself is a worthy subject for additional treatment by this author, or by others interested in REAL ID, as

well as those interested in immigration related policies generally, but is outside of the scope of this thesis.

A further limit on the research is that while the three case study states demonstrate a variety of approaches to REAL ID and a set of unique challenges, the way the three states have approached implementation, and their unique issues, can only demonstrate so much. Ideally, the author would have liked to undertake a case study of each of the states and territories and then grouped an analysis of those case studies into more significant trends, lessons learned, and best practices. The academic calendar and the ambitiousness of such a project put a check on the author's natural tendencies to want to tackle that issue. However, the *next* project is always available.

II. REAL ID AS A SOLUTION TO THE PROBLEM OF INSECURE IDENTITY DOCUMENTS

The REAL ID Act can be traced to the aftermath of 9/11, when it became apparent that the hijackers had acquired numerous licenses or identification documents from different states and used those documents to embed themselves into U.S. society, and ultimately, to board the aircraft used in the attacks. The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), in its principal report, and in the associated Staff Report entitled *9/11 and Terrorist Travel: A Staff Report of the National Commission on Terrorist Attacks upon the United States*, provided detailed information regarding the travel of the hijackers.³⁰ According to the 9/11 Commission, all the pilots, and 14 of the 15 operatives, had acquired one or multiple forms of state issued identification documents.³¹ As noted in the Staff Report, having those documents would have “assisted them in boarding commercial flights, renting cars, and other necessary activities.”³² (See Appendix A for a detailed listing of the state driver’s licenses and identification documents obtained by the 9/11 hijackers.) As a result of its findings, the 9/11 Commission made the following recommendation:

Recommendation: Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.³³

³⁰ National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, Authorized Edition (Westminster, MD: SOHO Books, as released by the U.S. Government, 2010).

³¹ National Commission on Terrorist Attacks upon the United States, *9/11 and Terrorist Travel: A Staff Report of the National Commission on Terrorist Attacks upon the United States* (Franklin, TN: Hillsboro Press, 2004), 13, 44.

³² National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 390.

³³ Ibid.

The REAL ID Act passed with no debate on its provisions, and was attached to a bill dealing with tsunami relief and military appropriations.³⁴ The easy part, it seems, was passing the law; the greater difficulty lay in maintaining consensus after its passage, when the Bush administration sought to implement the provisions through the federal rulemaking process, during which it received and addressed over 21,000 public comments.³⁵

The principal elements of REAL ID relate to standards that the law charged the federal government with promulgating for state-issued driver's licenses and identification cards to be accepted for an "official purpose."³⁶ The REAL ID Act defines "official purpose" as including accessing federal facilities, boarding federally regulated commercial aircraft, entry into nuclear power plants, and such other purposes as established by the Secretary Homeland Security.³⁷ DHS issued the final regulations on January 29, 2008.³⁸ They included standards on "the information and security features that must be incorporated into each card; application information to establish the identity and lawful status of an applicant before a card can be issued; and physical security standards for the locations issuing driver's licenses and identification cards."³⁹

The generally acknowledged purpose of such efforts was to address the myriad issues that arise from the increasing uncertainty that exists regarding the identity of the persons who interact with the government, with commercial systems, and with all

³⁴ Electronic Privacy Information Center, *REAL ID Implementation Review: Few Benefits, Staggering Costs: Analysis of the Department of Homeland Security's National ID Program*, 3.

³⁵ "Department of Homeland Security, Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10,819," Washington, D.C.: GPO, 2007, <http://www.gpo.gov/fdsys/pkg/FR-2007-03-09/html/07-1009.htm>; Department of Homeland Security, "Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. 5271," January 29, 2008, <http://www.gpo.gov/fdsys/pkg/FR-2008-01-29/html/08-140.htm>.

³⁶ EPIC: *Real ID Implementation Review*.

³⁷ *The REAL ID Act of 2005*, 312.

³⁸ Department of Homeland Security, "Final Rule."

³⁹ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*.

Americans in their daily lives or interact with others through identity theft.⁴⁰ Balanced against greater assurances of identity document security, and the true identity of those dealt with in society are the weighty concerns relating to information security, privacy, and liberty. REAL ID's enactment and the related implementation efforts have raised numerous questions including whether it serves to create a form of national ID, whether it raises substantial constitutional and privacy concerns, and whether acceptable alternatives exist.

The use of fraudulently obtained identity documents by several of the 9/11 hijackers is relatively well known, but it is not the only example. A report, prepared by the Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology and Homeland Security, shortly before the enactment of REAL ID illustrates the role that insecure documents play in national security concerns.

One area of concern to the Subcommittee is document security and terrorist use of identity theft . . . Since 1998, the Subcommittee has held seven hearings on identity theft and fraud. (citation omitted) During a Subcommittee hearing in 2002, Dennis Lormel, Chief of the FBI's Terrorist Financial Review Group, testified that identity theft was a 'key catalyst' for terrorist groups. (citation omitted) He said that identity theft posed an 'alarming' threat and that 'terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain . . . cover employment and access to secure locations.' (citation omitted)

It is clear from the GAO's report that terrorists and other dangerous criminals can pass as U.S. citizens or steal American identities with alarming ease. Robert Cramer, the Managing Director of the GAO, who oversaw the investigations, testified, 'The weaknesses we found during these investigations clearly show that border inspectors, motor vehicle departments, and firearms dealers need to have the means to verify identity and to determine whether out-of-state driver's licenses presented to them are authentic.' (citation omitted).

John Pistole, Acting Assistant Director of the FBI's Counterterrorism Division, said that terrorists have long committed identity theft and misused Social Security numbers to infiltrate the United States. (citation omitted) Social Security number fraud has enabled them 'to obtain such

⁴⁰ The Institute for Communitarian Policy Studies, George Washington University, "Communitarian Update #48» Institute for Communitarian Policy Studies," September 24, 2002, <http://icps.gwu.edu/contact/mailling-list/communitarian-letter-archives/communitarian-update-48/>.

things as cover employment and access to secure locations.’ (citations omitted) Once Social Security numbers and driver’s licenses are obtained, bank and credit-card accounts, through which terrorism financing is facilitated, are easily accessed. (citations omitted)

Chairman Kyl said that the GAO’s investigation ‘shows a dangerous lapse in the ability of state and federal employees to detect and deter document fraud, which is often the first step terrorists must take to assimilate themselves in the United States and form sleeper cells.’⁴¹

The final regulations issued by DHS on January 29, 2008, included standards on “the information and security features that must be incorporated into each card; application information to establish the identity and lawful status of an applicant before a card can be issued; and physical security standards for the locations issuing driver’s licenses and identification cards.”⁴²

A. THE REAL ID DOCUMENT SECURITY ELEMENTS

Under the REAL ID Act, the states must adhere to the federally developed standards in their issuance of state-issued driver’s licenses and identification cards in order for their state issued documents to be accepted for an “official purpose” under the Act.⁴³ The final regulations issued by DHS included, among other things, standards on “the information and security features that must be incorporated into each card.”⁴⁴ That requirement was intended to make the documents themselves more secure and tamperproof. In that regard, REAL ID requires that state issued driver’s licenses and identification documents contain the following elements.

⁴¹ *United States Senate Committee on the Judiciary Subcommittee on Terrorism, Technology, and Homeland Security: Three Years After September 11: Keeping America Safe* (Washington, DC, March 2005).

⁴² Department of Homeland Security, *Final Rule*; Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*.

⁴³ Department of Homeland Security, *Final Rule*. The REAL ID Act defines “official purpose” as including accessing federal facilities, boarding federally regulated commercial aircraft, gaining entry into nuclear power plants, and such other purposes as established by the Secretary of Homeland Security.

⁴⁴ *Ibid.* In general, the requirements upon the states fell within three general areas: 1) certain information that must be contained within the documents, 2) certain issuance standards for the documents, and 3) certain other practices that states were required to adopt that generally addressed the integrity of the issuance process.

- The person's full legal name
- The person's date of birth
- The person's gender
- The person's driver's license or identification card number
- A digital photograph of the person
- The person's address of principal residence
- The person's signature
- Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes
- A common machine-readable technology, with defined minimum data element⁴⁵

Balanced against greater assurances of identity document security and the true identity of those dealt with in society, are the weighty concerns relating to information security, privacy, and liberty. DHS entered the debate in a significant way with the introduction and passage of the REAL ID Act. REAL ID, as it has become known, has come under assault by a number of states, which have resisted its implementation on multiple grounds, including as an unfunded mandate, as an intrusion into state sovereignty, and as the creation of an insecure national ID system that imperils the privacy of their citizens. This thesis elaborates on those various concerns in subsequent chapters.

This chapter discusses the changes REAL ID sought to make to improve the security of state identification documents, and also puts REAL ID into context by discussing how REAL ID fits into the recent federal efforts to address the integrity of identification documents. REAL ID represents a significant, bold, and controversial step by the federal government to address document security. However, it is not the first time that the federal government had sought to address the problem of insecure identity documents through the setting of standards. Two previous, recent legislative efforts are worth noting.

⁴⁵ *The REAL ID Act of 2005*, Section 202(b).

B. DOCUMENT SECURITY AND PREVIOUS LEGISLATIVE EFFORTS, DOCUMENT SECURITY PROVISIONS OF IIRIRA

Concerns about the security of identity documents preceded the experience of 9/11. One previous effort, and an early precursor of REAL ID, came with Congress' passage of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, known as (IIRIRA).⁴⁶ While largely focused on immigration reforms, it contained a provision related to document security—Section 656(b) entitled State-Issued Driver's Licenses and Comparable Identification Documents. That provision, like REAL ID, required federal agencies only to accept documents as proof of identity that conformed to federally established requirements for secure documents. In the case of IIRIRA, those standards were to be set forth in regulations issued by the Secretary of Transportation.⁴⁷ The document security provision had three basic elements. First, applicants for driver's licenses and identification cards would be required to submit such documents for verification of identity as required by regulations issued by the Secretary of Transportation, following consultation with the American Association of Motor Vehicle Administrators (AAMVA).⁴⁸ Second, the driver's license or identification documents were to be in a form consistent with requirements set forth in regulations promulgated by the Secretary of Transportation, again after consultation with AAMVA. In general, the documents were to contain security features designed to limit tampering, counterfeiting, photocopying, or otherwise duplicating, the driver's license or identification document for fraudulent purposes and to limit their use by imposters. Third, the state driver's licenses and identity documents were to include an electronic version of the Social Security number (SSN), unless certain conditions were met to include verifying the SSN with the Social Security Administration.⁴⁹ The Department of Transportation (DOT)

⁴⁶ *The Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, Public Law 104–209, Div. C, 110 Stat. 3009, 1996, REAL ID Public Law.pdf.

⁴⁷ *Ibid.*, Section 656(b)(1)(A)(iii).

⁴⁸ AAMVA, which is an association of the nation's motor vehicle administrators, has been an active and vocal advocate for the need to improve the security of state driver's licenses and identity documents. It is generally recognized that its report, issued in 2004, *AAMVA DL/ID Security Framework*, was a significant influence on the passage of REAL ID.

⁴⁹ *The Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, Section 656; Garcia, Lee, and Tatelman, *Immigration*, 38. See footnote 117.

published a Notice of Proposed Rulemaking (NPRM) on June 17, 1998, to implement the document security provisions. The proposed rule also provided that states would be required to self-certify by October 1, 2000, that they were in full compliance with the regulations.⁵⁰

In addition to the security features, and provisions related to the SSN issues, the proposed rule required the submission of one primary document and one secondary document. The primary documents would establish identity, and the secondary documents would be used to help to verify or confirm that identity. It was DOT's intention to publish the list of acceptable documents as appendices to the final rule and update them as necessary through subsequent Federal Register notices.⁵¹

However, the document security provisions proved to be very controversial, due to concerns that it appeared to establish a national ID system, and Congress withheld funding necessary for implementing the provisions.⁵² The DOT never issued a final rule and the law's provisions were never implemented. Instead, Congress repealed the document security provisions of IIRIRA in 1999, and two years later, DOT withdrew the proposed rule providing the following explanation.

The agency received a total of 2,591 comments, the vast majority of which strongly opposed the agency's proposal. The most frequent objections were based on privacy and civil liberty concerns. Congress also received an overwhelming number of negative comments regarding section 656(b) and the agency's proposal to implement that section. On October 9, 1999, Congress repealed section 656(b) Pub. L. 106-69, 113 Stat. 1027. Accordingly, the proposed rule to implement the requirements contained in section 656(b), published on June 17, 1998, at 63 FR 33220, entitled State-Issued Driver's Licenses and Comparable Identification Documents, is hereby withdrawn.⁵³

⁵⁰ Department of Justice, "Department of Transportation, Notice of Proposed Rulemaking: State Issued Driver's Licenses Minimum Standards for Driver's Licenses and Comparable Identification Documents, 63 Fed Reg. 33,220," June 17, 1998, http://www.justice.gov/eoir/vll/fedreg/1998_1999/fr17jn98P.pdf.

⁵¹ Ibid.

⁵² Garcia, Lee, and Tatelman, *Immigration*, 38. See footnote 117.

⁵³ U.S. Government Printing Office, "Department of Transportation, Withdrawal of Proposed Rule on State-Issued Driver's Licenses and Comparable Identification Documents 66 Fed Reg, 56261," November 7, 2001, <http://www.gpo.gov/fdsys/pkg/FR-2001-11-07/html/01-28007.htm>.

C. DOCUMENT SECURITY PROVISIONS OF ITRPA

The second, and more substantial effort, which served as the immediate predecessor to REAL ID, was the effort to establish standards contained in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). An important section of the IRTPA was dedicated to implementing the recommendation of the 9/11 Commission that the federal government establish federal standards for the issuance of driver's licenses personal identification documents, SSNs, and birth certificates. The House and Senate versions of the legislation took very different approaches to the issue with the House of Representatives setting forth specific requirements in the proposed legislation, and the Senate version electing to require that the issue be placed under federal regulation, but leaving it to the specific federal agencies to determine the appropriate form that the regulatory efforts should take.⁵⁴ While the proceedings in Congress surrounding the standards were contentious, the final version of the legislation contained elements of both, although many of the more controversial provisions were left out of the final version, with members indicating that they would be revisited during the next Congress.⁵⁵

The IRTPA again delegated authority to the Secretary of Transportation, but this time, in consultation with the Secretary of Homeland Security, to issue regulations setting minimum standards for federal acceptance of state issued driver's license and identity cards.⁵⁶ In many respects, the law's provisions were very similar to REAL ID with the documents being required to incorporate the following data elements pursuant to section 7212 (b)(2)(D).

- The person's full legal name
- The person's date of birth
- The person's gender
- The person's driver's license or personal identification card number

⁵⁴ Todd B. Tatelman, "Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates," January 6, 2005, <http://www.fas.org/irp/crs/RL32722.pdf>.

⁵⁵ Ibid.

⁵⁶ Ibid., 2.

- A digital photograph of the person
- The person's address of principal residence
- The person's signature⁵⁷

It also required that regulations be issued within 18 months and prohibited acceptance of state documents for a "federal official purpose" that within two years of enactment did not meet the regulatory requirements that included the following additional factors.

- Use of a machine readable technology
- Tamperproof features on the card
- Standards for documentation, and verification
- Processing of the applications

Some key differences with REAL ID included language that prohibited the federal government from not only infringing upon the "State's power to set criteria concerning what categories of individuals are eligible to obtain a driver's license or personal identification card from that State," but also from requiring a state to take an action that "conflicts with or otherwise interferes with the full enforcement of state criteria concerning the categories of individuals that are eligible to obtain a driver's license or personal identification card."⁵⁸ This provision would, understandably, be welcomed by states that feared federal intrusion into what they would consider to be state functions.

Another key difference that did not survive in REAL ID, and which has contributed to some of the state rebellion against that law, was the inclusion in IRTPA of a provision, recommended by the Senate, of negotiated rulemaking between the federal government and the states. According to the Congressional Research Service's (CRS) analysis of IRTPA.

This process is designed to bring together agency representatives and concerned interest groups to negotiate the text of a proposed rule. The rulemaking committee is required to include representatives from: (1) State and local offices that issue driver's licenses and/or personal

⁵⁷ *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-408 §§ 7211-7214, 118 Stat. 3638, 3825-3832 (2004).

⁵⁸ Tatelman, "Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates," 3.

identification cards; (2) State elected officials; (3) Department of Homeland Security; and (4) interested parties.⁵⁹

The negotiated rulemaking was to develop recommendations within nine months, while assessing the benefits and costs of the recommendations, and thereafter, publishing a final rule within 18 months of the law's enactment.⁶⁰

In addition to dealing with the security of state driver's licenses and identity documents, the IRTPA took measures to address the security of two additional categories of documents, birth certificates and Social Security cards. With respect to birth certificates, the IRTPA delegated authority to the Secretary of Health and Human Services to establish standards no later than one year from the date of enactment for such documents to be acceptable for federal purposes, but the provisions would not be binding on the states until two years later. The standards would require adoption of a variety of measures, ranging from the use of safety paper, to measures to verify the information provided, and additional steps for people not applying for their own birth certificate.⁶¹ Interestingly, and in an apparent attempt to make clear that the federal government was not taking over the role played by the states, the legislation specifically stated that uniformity would be not required in the appearance of the birth certificates, and also allowed for differences in how the birth records were stored, and subsequently, used to produce birth certificates.⁶² The IRTPA also included language that authorized grants to assist the states to meet the standards.⁶³ It further offered a two-year extension from consequences from their failure to comply, for those states making "reasonable efforts" to achieve compliance.⁶⁴

⁵⁹ Tatelman, "Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates," 3.

⁶⁰ Tatelman, "Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates."

⁶¹ *Ibid.*, 9.

⁶² *Ibid.*

⁶³ Tatelman, "Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates."

⁶⁴ *Intelligence Reform and Terrorism Prevention Act of 2004*, Section 7212(d).

Turning to the IRTPA's changes to the Social Security card, a number of modifications were made regarding the verification, display, and use of the SSN to reduce fraud risks associated with them. The primary changes were that the Commissioner of the Social Security Administration (SSA) was to prohibit the issuance of more than three replacement Social Security Cards in one year to individuals, or a total of 10 during the individual's lifetime, unless the Commissioner determines a minimal risk of fraud is present.⁶⁵ In addition, requirements were imposed to increase the verification of information submitted in support of a request to establish eligibility for an original or replacement Social Security card, as well as requiring independent verification of all information submitted by applicants for SSNs.⁶⁶ A number of measures were included in the law to increase the protection of the SSNs and deter their fraudulent use. Among them, were the creation of an interagency task force, which would be responsible for developing requirements for safeguarding SSN information, verifying its authenticity, and developing enforcement mechanisms to deter its fraudulent issuance or use of SSN and Social Security cards.⁶⁷ Specific provisions were also included to address the special problem of fraud associated with SSNs related to newborns, with reports and requirements to submit recommendations to Congress. Finally, on a more basic level, to address identity theft and protect privacy, IRTPA also prohibited states and local political subdivisions from displaying the SSN in electronic or other format on the driver's licenses, identity documents, or other forms of identification issued by the states or their subdivisions.⁶⁸

1. Status of IRTPA Document Security Provisions

It appears that IRTPA achieved some success as to the changes associated with the security of the Social Security card. The Office of the Inspector General (OIG) of the SSA undertook an audit and released its findings and recommendations in a report

⁶⁵ Tatelman, "Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers' Licenses, Social Security Cards, and Birth Certificates," 6.

⁶⁶ Ibid., 5.

⁶⁷ Ibid., 6–7.

⁶⁸ Ibid., 7.

completed in 2008. It generally was pleased with the SSA's progress but recommended that SSA periodically assess its efforts and make adjustments as needed.⁶⁹

D. CONCLUSION

The terrorist attacks of 9/11 drove home with startling urgency the need to address a number of vulnerabilities faced by the nation in a number of areas that imperiled its national security. Among those, was the relative ease with which individuals could obtain identity documents that would allow them to remain in the United States and engage in activities that could facilitate events like 9/11. The United States had not been oblivious to these issues, and has been grappling with, and seeking to address, the relative insecurity of driver's licenses and identity documents by strengthening the security of the documents and verification measures associated with their issuance to address fraud and identity theft concerns. While measures were pursued both before and after 9/11 through measures such as IIRIRA and IRTAPA, it took the events of 9/11 to galvanize government efforts to address this vulnerability in a more comprehensive manner.

An examination of the previous efforts shows that provisions in those earlier legislative efforts recognized the role of the states in identity document issuance and sought to balance the role of the federal government with that of the states; as best seen with the negotiated rulemaking provisions contained in the IRTPA. It is unclear what would have resulted had those efforts been allowed to proceed. On the one hand, they may have resulted in weaker document security provisions, thus diminishing the effort to address fraud. It may have also led to endless debate and disagreement with ensuing delays, which would have delayed implementation of needed changes. On the other hand, had the discussions been successful, it is easy to see how the states—particularly the ones currently opposing REAL ID—might have been more accepting of the changes and could have facilitated implementation and reduced state resistance.

⁶⁹ Office of the Inspector General, Social Security Administration, "Audit Report: The Social Security Administration's Compliance With Intelligence Reform and Terrorism Prevention Act of 2004 Provisions Regarding Security of Social Security Cards and Numbers," May 2008, <http://oig.ssa.gov/sites/default/files/audit/full/html/A-08-08-18058.html>.

REAL ID appears to have been one of those legislative enactments that passed due to all of the elements coming together to enable its passage, where it might not have passed at another time, and it seems it likely it would not be passed today. Furthermore, the Bush administration acted swiftly for a legislative and regulatory scheme of such a broad scope and tremendous impact upon the states and territories and their citizens. It undertook and published an extensive and ambitious rulemaking process in what many would agree was record time when compared with the difficulty and slow pace of extensive rulemaking efforts. It processed and addressed over 21,000 public comments and published regulations that altered significantly the requirements to be met by states in their identity document issuance procedures. As challenging as the rulemaking effort was, the more substantial challenges for both the federal government and the state governments, involved taking the measures necessary to implement the law successfully and do so in a way cognizant of, and which addressed the various concerns associated with REAL ID. The most significant of those concerns and the controversies surrounding them are discussed in the chapters that follow.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DOES REAL ID CREATE A NATIONAL ID?

The literature review has briefly touched on several of the reasons that the passage and implementation of REAL ID has proven to be controversial. Among them, were issues, such as Tenth Amendment concerns regarding the proper role of the federal government as to functions reserved for and better entrusted to the states, concerns regarding the implementation costs of REAL ID and the belief that the law set forth unfunded mandates for the states, and privacy and civil liberties concerns stemming from the law's requirements. All these reasons will be the subject of more detailed discussions in the paper. Within the category of concerns stemming from violations of civil liberties, is the concern raised by critics that REAL ID establishes a national identity card (national ID). This assertion composes part of the debate that continues to this day. DHS became enmeshed in the national ID debate through its efforts to implement REAL ID, which was enacted a mere two years after DHS came into existence. That law has come under assault by many who object to what they view as the creation of an insecure national ID system that imperils the privacy and civil liberties of the citizenry.⁷⁰

This chapter discusses DHS' response to claims that it was establishing a national ID, and compares the REAL ID elements that give rise to the charge that it creates a national ID, to the efforts to those of four key democracies, the United Kingdom, India, South Africa, and Germany that have implemented, or have tried but failed to implement national ID schemes. Doing so provides a better understanding of how U.S. efforts compare to those of countries that have actually sought to establish a national ID. This thesis finds that the U.S. effort is more modest in its design, and discusses how DHS has countered the assertion that REAL ID establishes a national ID system. Nevertheless, REAL ID has faced opposition and slow adoption by many states. Looking at the experience of countries that have sought to implement a national ID system can assist DHS in identifying best practices that can help address some of the social acceptance

⁷⁰ EPIC: *Real ID Implementation Review*; see also Steinbock, "Fourth Amendment Limits on National Identity Cards," in *Privacy and Technologies of Identity: A Cross-disciplinary Conversation*. (Steinbock cites in footnote 1 to various articles from the last 20 years in which conversations regarding national IDs are referenced.).

issues that are impeding full implementation of the law, as well as countering critics' claims that REAL ID constitutes a national ID scheme.

A. WHAT CONSTITUTES A NATIONAL ID?

The definition of a national ID is itself controversial, and a lack of consensus exists as to whether the United States has been moving toward a national ID scheme. Some view a national ID document as establishing both citizenship and identity. By that definition it would appear that the only document that establishes both in the United States is the passport.⁷¹ Others assert that the use of the phrase “national ID” is “a bit of a misnomer in that a card would likely be but one component of a large and complex nationwide identity system, the core of which would be a database of personal information on the U.S. population.”⁷²

If REAL ID in its present form does not establish a national ID, then it begs the question of what does constitute a national ID? Little consensus may exist on this issue as well, but some sources point to the treatment of this issue by Roger A. Clarke, who is credited with having articulated the “seminal formal definition” of a national ID.⁷³ Most recently, Clarke has identified several elements necessary to establish a national ID, and which, taken together, illustrate the complexity of national identification schemes. Those elements, are listed as follows.

- A database
- A Unique Signifier for Every Individual either a unique number or a biometric identifier)
- An “(Id)entification token” such as an ID card
- Quality assurance mechanisms

⁷¹ Ruth Ellen Wasem, *Unauthorized Aliens' Access to Federal Benefits: Policy and Issues*, CRS Report RL34500 (Washington, DC: Congressional Research Service, September 17, 2012), 3.

⁷² Stephen T. Kent et al., *IDs--Not That Easy Questions about Nationwide Identity Systems* (Washington, DC: National Academy Press, 2002), <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=87005>.

⁷³ A. Michael Froomkin, “The Uneasy Case for national ID Cards,” in *Securing Privacy in the Internet Age*, ed. Anupam Chander, Lauren Gelman, and Margaret Jane Radin (Stanford, CA: Stanford Law Books, 2008), citing to Roger A. Clarke, “Human Identification in Record Systems” (June 1989) and Roger A. Clarke, “The Resistible Rise of the National Personal Data System,” 5 *Software L. J.* 29, 33–36 (1992).

- Widespread use of the data flows, the identifiers and the database
- Obligations on individuals and many organizations
- Sanctions for non-compliance⁷⁴

1. United States-REAL ID

From the beginning, opponents have claimed that REAL ID established a national ID requirement for the United States. The Bush administration denied the charge and sought to address that concern through the rulemaking process. As part of that process, DHS issued a PIA, on January 11, 2008, to accompany the implementing regulations for REAL ID.⁷⁵ This issuance was done in accordance with subsection 4 of Section 222 of the Homeland Security Act of 2002, as amended, which requires the DHS Chief Privacy Officer to conduct a “privacy impact assessment of proposed rules of the Department.”⁷⁶ This PIA was an update to one published in March 2007 that accompanied the Notice of Proposed Rulemaking (NPRM). In the final rule PIA, DHS directly addressed five privacy areas posed by REAL ID.⁷⁷ It specifically recognized the national ID concern raised by commenters during the NPRM period, stating: “[a] primary privacy concern has been whether the REAL ID will result in a national identity system, including a centralized database of PII including all drivers.”⁷⁸ DHS refuted the claim by stating that while it could not control what use the states would make of the identity cards, DHS could nonetheless assure the public regarding the centralized database that “[n]either the REAL ID Act nor the requirements of the final rule expressly create a centralized database of all drivers’ information.”⁷⁹ DHS further noted that the preamble to the rule stated:

⁷⁴ Roger A. Clarke, “National Identity Schemes—Elements,” February 8, 2006, <http://www.rogerclarke.com/DV/NatIDSchemeElms.html>.

⁷⁵ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*.

⁷⁶ *The Homeland Security Act of 2002*, Public Law 107–296, 116 Stat. 2135 2002, <http://www.gpo.gov/fdsys/pkg/BILLS-107hr5005enr/pdf/BILLS-107hr5005enr.pdf>.

⁷⁷ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*, 3.

⁷⁸ *Ibid.*, 6.

⁷⁹ *Ibid.*

DHS does not intend that a REAL ID document become a de facto national ID based on the actions of others outside of DHS to limit their acceptance of an identity document to a REAL ID-compliant driver's license or identification card.⁸⁰

The PIA provided, however, that even though no central database would exist, REAL ID's prohibition on states issuing a REAL ID compliant driver's license to someone who holds a driver's license from another state (without verifying that the license has been or is in the process of being terminated), made it necessary to facilitate the states' ability to verify that fact. Consequently, while no *central* repository was established, it was necessary for the states to be able to utilize an "index or pointer system rather than checking with each State DMV individually."⁸¹ The PIA goes on to explain that without such a pointer system, it would be cost prohibitive for states to undertake the required verification and they would be inundated by data if they were required to exchange information based only on individual queries. Nevertheless, DHS' Chief Privacy Officer noted in the PIA that DHS would work with the states to ensure that

this central repository is only used to facilitate the State-to-State data checks or to permit access by authorized law enforcement personnel who are checking a specific license or identification card against the system and for no other purpose. The access rules to the still-to-be-built hub, for example, will help implement these protections. In addition, DHS will work to ensure that this index or pointer system will include the minimal amount of PII needed to facilitate effective querying and reduce the occurrence of false positives and false negatives.⁸²

In addressing additional concerns about the use to which information in the hub (the personally identifiable information, or PII), might be utilized, the PIA further provided:

Of particular privacy concern, however, is how the PII contained in the State-to-State data verification index or pointer system will be used by DHS, the States, or other entities, if, given access to it. Setting limitations on the use of the PII in the index should be the first item of business for the governance body established to operate and oversee the State-to-State

⁸⁰ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*, 6.

⁸¹ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act: In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, March 1, 2007, 6–7.

⁸² *Ibid.*, 7.

data verification system. The Privacy Office intends to monitor the work of the governance body and to provide privacy guidance as appropriate. The central index or pointer system should not be used, for example, by any Federal or State agency for intelligence, data mining, or “fishing expeditions.” Rather, access should be limited to targeted law enforcement or DMV investigations or verification of an individual’s identity based on a “need to know,” as outlined in the Privacy Act and many similar State privacy acts.⁸³

Thus, DHS sought to address directly what the major concerns would be regarding the use of PII associated with the REAL ID verification system. It also sought to assure the public it was cognizant of the concerns and was taking action to ensure that the information was not used for purposes that traditionally evoke concerns about national ID systems. At the same time, it sought to give states autonomy and responsibility for the use of information.

Overall, there has been a lack of consensus on REAL ID’s status as a national ID, with some advocates insisting that the federal government was setting up such a program, and other advocates arguing that no national ID system was established, but that national security concerns required the federal government to develop standards for state identity documents. Even if the REAL ID framework itself does not actually establish a national ID, some assert that implementing REAL ID may make a move toward a national ID system more likely.⁸⁴

A range of views exists as to whether the standards imposed by REAL ID in essence create a national ID. On one side, are the civil rights/civil liberties advocates such as the EPIC, which assert that REAL ID represents an effort to establish a national ID, despite historical and recent congressional opposition to such a system, reaffirmed by Congress when it established DHS.⁸⁵ On the other end of the spectrum are individuals and entities that strongly support REAL ID and reject the national ID charge, noting that implementing the law requires no aggregation of data into a centralized database operated

⁸³ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act*, 11.

⁸⁴ Steinbock, “Fourth Amendment Limits on National Identity Cards,” in *Privacy and Technologies of Identity: A Cross-disciplinary Conversation*.

⁸⁵ EPIC: *Real ID Implementation Review*.

by the federal government.⁸⁶ Nevertheless, among supporters of REAL ID, outspoken advocates of a national ID system do exist, who see direct and indirect benefits of secure identity documents to further national security and the prevention of terrorism.⁸⁷

Interestingly, among the supporters of a national ID system is the *Washington Post*, which responded to the issue most recently in the context of the debate over comprehensive immigration reform. The *Post*, a moderate to liberal newspaper, supports immigration reform, and has come out in favor of adopting a tamper proof national ID card incorporating biometrics, such as a fingerprints or a comparable identifier, and noted that the President and a bi-partisan group of senators had urged something similar while not calling it a national ID.⁸⁸ In response to the criticism that such a system would constitute intrusive government that threatens privacy, the *Post* offered the following response.

Critics on both the civil-liberties left and the libertarian right have long resisted such cards as the embodiment of a Big Brother brand of government, omniscient, invasive and tentacular. Their criticisms ring hollow.

More than a third of Americans (35 percent) possess passports; up from just 6 percent 20 years ago — and all passports issued since 2007 contain chips that enable biometric use of facial recognition technology. The proliferation of passports for foreign travel has not encroached on Americans' civil liberties. Why would another form of ID, used for employment verification, pose such a threat?

Yes, unscrupulous employers could still ignore the law, but doing so would become riskier and more prone to enforcement. Critics contend that a national ID would only drive up the cost of counterfeit documents. Would they prefer that falsified documents are cheap?⁸⁹

⁸⁶ Center for Immigration Studies, "Repealing REAL ID? Rolling Back Driver's License Security (Announcement)," accessed September 3, 2013, <http://www.cis.org/realidannounce>.

⁸⁷ Dershowitz, "Thinking About National ID Cards"; see also, David Frum and Richard Norman Perle, *An End to Evil: How to Win the War on Terror* (New York: Ballantine, 2004).

⁸⁸ Editorial Board, "The Case for a national ID Card," *The Washington Post*, sec. Opinions, February 2, 2013, http://www.washingtonpost.com/opinions/the-case-for-a-national-id-card/2013/02/02/49d4fb80-6cb5-11e2-ada0-5ca5fa7ebe79_story.html.

⁸⁹ Ibid.

While the debate continues, it is unlikely that consensus on whether REAL ID constitutes a national ID can be reached, those who support enhanced identity documents believe that such a system could prevent tragedies like 9/11 because in addition to the biographic information contained on the cards, they could be equipped with a chip through which an embedded fingerprint or other biometric identifier could then be compared with the corresponding biometric of the person presenting the document to verify identity. In addition, information about the individual maintained in law enforcement, immigration databases, or watch lists could be associated with the person.⁹⁰

2. Understandable Concerns Are Raised by a National ID

Regardless of an individual's opinion on the issue of national ID systems, it is easy to understand the concerns surrounding them, which relate principally to privacy and the loss of liberty. One author who set out to examine the societal perceptions of biometric technology and what is necessary to promote acceptance, describes the concern as follows.

Foremost among these are the loss of liberty, whether in the form of governmental control or the misuse of information, and the potential for loss of privacy and anonymity; all of which must be offset by the legitimacy of identification.⁹¹

The author summarizes the challenge for DHS and any entity seeking to improve identification systems—whether or not one calls them a national ID system—as follows.

Societal acceptance or rejection can shore up a system of identification or destroy it. The societal assessment of the objectives of a system of identification in the public or private sector is no easy matter, yet it is safe to say that ignoring the political, societal, and cultural influences that shape perceptions of systems of identification is impossible.⁹²

⁹⁰ Tova Andrea Wang, *The Debate Over a National Identification Card* (The Century Foundation Homeland Security Project, May 10, 2002).

⁹¹ Lisa S. Nelson, *America Identified: Biometric Technology and Society* (Cambridge, MA: The MIT Press, 2011), 13, <http://books.google.com/books?id=64zo8GjybdYC&printsec=frontcover&dq=America+Identified&hl=en&sa=X&ei=k7cRUtKnEKugyAHy3IEo&ved=0CC8Q6AEwAA#v=onepage&q=America%20Identified&f=false>.

⁹² *Ibid.*, 56.

The societal acceptance issue that DHS has faced with REAL ID becomes apparent when one considers that society is generally willing to support systems of identification when it is facing issues, such as “[e]xternal threats of war, identification of criminal elements in society, distribution of social welfare, and internal threats to social stability such as immigration.”⁹³ Yet, public support and acceptance wanes when the idea of long-term reliance on identification systems for “day-to-day bureaucratic workings of the government” is the goal.⁹⁴ Part of the difficulty facing REAL ID is that the effort to increase the security of state identity documents is, on one hand, an effort to address an external threat of terrorism and criminality, while at the same time, it impacts what is seen as a day-to-day bureaucratic activity—the routine process of getting and using state licenses and identity documents. In addressing public concerns and being able to distinguish REAL ID efforts from efforts more clearly intended to establish a national ID, it is helpful to examine the experiences of other countries to see if any lessons can be learned for DHS and the states.

B. NATIONAL ID EFFORTS IN COMPARISON COUNTRIES

Four countries that have adopted or are seeking to adopt a national ID system were selected for comparison purposes with U.S. efforts on REAL ID. Each represents a western style democracy that brings unique considerations to the analysis and has faced similar considerations in its implementation efforts. The United Kingdom (UK) was selected because of its status as a close U.S. ally, and as an example of a nation that has alternatively succeeded and failed at implementing a national ID system. India was selected as a country that has embarked on an effort to issue a national ID to an extremely large population and has done so under challenging circumstances given the population size, and the remoteness of some areas of the country, and has leveraged private enterprise in its implementation challenges. South Africa was selected as it is considered “the first example of a “truly biometric order” where “[m]uch of what the advocates of biometric registration systems around the world have been calling for since the start of

⁹³ Nelson, *America Identified: Biometric Technology and Society*, 13.

⁹⁴ *Ibid.*

the War on Terror has already been implemented.”⁹⁵ Finally, Germany was selected as the classic example of the use of identity controls by the government to harm segments of its population, yet has overcome that history and today has a national ID system in place.

1. The United Kingdom

The United Kingdom represents an interesting case study with its alternating adoption of, and rejection of national IDs. It is unusual within Europe for not having a national ID.⁹⁶ This situation has not always been the case as the United Kingdom had two previous experiences with national ID’s prompted by war related considerations. During World War II, for example, the United Kingdom enacted the National Registration Act of 1939, which required all residents to carry an identity card for the duration of the war “emergency.”⁹⁷

Its ambivalence regarding a national ID system was most recently manifested in the government’s actions surrounding the Identity Act of 2006 (Identity Act).⁹⁸ The concept behind the Identity Act was to link the individual to a biometric identifier in the form of fingerprints, and in turn, link that information to the National Identity Register.⁹⁹ The United Kingdom started issuing IDs in 2009.¹⁰⁰ However, it repealed the law less than two years later through passage and enactment of the Identity Documents Act on January 21, 2011.¹⁰¹ The repeal was a consequence of the 2010 national elections, when

⁹⁵ Keith Breckenridge, “The Elusive Panopticon: The HANIS Project and the Politics of Standards in South Africa,” in *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, ed. Colin J. Bennett and David Lyon (London; New York: Routledge, 2008), 287.

⁹⁶ David Wills, “The United Kingdom Identity Card Scheme,” in *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, ed. Colin J. Bennett and David Lyon (London; New York: Routledge, 2008), 163.

⁹⁷ C. H. Rolph, “The English Identity Cards,” in *National Identification Systems: Essays in Opposition*, ed. Carl Watner and Wendy McElroy (Jefferson, NC: McFarland & Co., 2004), 125.

⁹⁸ Wills, “The United Kingdom Identity Card Scheme.”

⁹⁹ BBC, “In Full: Smith ID Card Speech,” sec. UK Politics, March 6, 2008, http://news.bbc.co.uk/2/hi/uk_news/politics/7281368.stm.

¹⁰⁰ Home Office, “Commencement of the Identity Cards Act 2006—Issue of Identity Cards and New Criminal Offences—Publications—GOV.UK,” accessed August 25, 2013, <https://www.gov.uk/government/publications/commencement-of-the-identity-cards-act-2006-issue-of-identity-cards-and-new-criminal-offences>.

¹⁰¹ Home Office, “ID Cards No Longer Valid—News Stories—GOV.UK,” January 21, 2011, <https://www.gov.uk/government/news/id-cards-no-longer-valid>.

a coalition of the Conservative Party and the Liberal Democrats agreed to repeal the 2006 legislation. One notable and dramatic action taken as a consequence of the repeal was that 500 hard drives housing the identity register were shredded to fulfill the requirement of the repeal legislation that the national register be destroyed.¹⁰²

The UK's recent attempt to establish a national ID was justified by the government on the basis of two main objectives. These objectives were set forth in a speech delivered by Home Secretary Jacqui Smith, on March 6, 2008.¹⁰³ The speech, intended to inject new momentum into the program's implementation, began from the premise that the National Identity Scheme was a public good, offering British citizens a new, secure, and convenient way to protect and prove their identity, and for the government, it was a way to support national security efforts.¹⁰⁴ The Home Secretary articulated the need as follows.

We all need to be able to prove who we are - quickly, easily and securely. And so it is essential for all of us to be able to lock our identity to ourselves and to protect its integrity. We need a way of doing so that we can trust in, and that can be trusted by others - when applying for a job, travelling abroad, or using business and government services.

As citizens, it will offer us a new, secure and convenient way to protect and prove our identity. And it will provide us with the reassurance we need that others who occupy positions of trust in our society are who they say they are as well.

As a government, we have a duty to ensure that the National Identity Scheme supports our national security, and that it provides a robust defence against those who seek to use of false identity to mask criminal or terrorist activity.¹⁰⁵

While the justification sounds quite similar to justifications in support of REAL ID, one notable difference is that the recently repealed UK national ID effort utilized a card that

¹⁰² Electronic Frontier Foundation, "Success Story: Dismantling UK's Biometric ID Database," accessed August 25, 2013, <https://www EFF.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database>.

¹⁰³ BBC, "In Full."

¹⁰⁴ Ibid.

¹⁰⁵ Ibid.

was linked to a national identity register. The card itself was to resemble the UK driver's license, but would hold more data, including two fingerprints and a photograph, that would be encoded on a chip.¹⁰⁶ The unique number and the chip facilitate linkage to the national identity register that the enabling legislation authorized to maintain additional information.¹⁰⁷ It was also anticipated that the document could be used, similar to a passport, to facilitate travel throughout Europe.¹⁰⁸ While the card was originally envisioned as mandatory, it was later made voluntary to address critics' concerns.¹⁰⁹ Its rollout was to have begun with transportation sector workers, followed by others in positions of public trust, such as Olympic security workers, and those working in critical infrastructure positions, such as power plants. It was next to have been made available on a voluntary basis to young people, beginning in 2010.¹¹⁰ Although the rollout began in Manchester, with the intention of expanding nationwide during 2011–2012, it did not extend beyond Manchester before being cancelled.¹¹¹

The opponents seized upon the program's mandatory nature, and disputed the government's stated reasons in support of the identity program, asserting:

[A] designer piece of plastic is not going to combat identity fraud, crime or terrorism. This intrusive scheme should be scrapped immediately."¹¹² Even the government's attempts to make it mandatory for airport workers failed, with the government backing off of even that requirement. The opposition also included a privacy rights group No2ID, which proved to be a vocal opponent. In addition, national polling suggested little support for the voluntary program.¹¹³ The cost of the program was also of concern, with the London School of Economics issuing a report finding that while the concept of a national identity system was supportable, the

¹⁰⁶ BBC, "UK's national ID Card Unveiled," sec. UK Politics, July 30, 2009, <http://news.bbc.co.uk/2/hi/8175139.stm>.

¹⁰⁷ Ibid.

¹⁰⁸ Ibid.

¹⁰⁹ Ibid.

¹¹⁰ BBC, "In Full."

¹¹¹ BBC, "UK's national ID Card Unveiled."

¹¹² Ibid.

¹¹³ Ibid.

current proposals were not feasible with the benefits not outweighing the costs.¹¹⁴

Critics also raised concerns about the security of the data and its ability to be compromised. In response, the government decided to build separate databases keeping the biographic details separate, physically and technologically, from the biometric data, consisting of fingerprints and photographs.¹¹⁵ This measure was taken to reassure the public that it was taking measures to mitigate the risks.¹¹⁶ In addition, the government stressed that the information would not be susceptible to hacking because the databases would not be available online.¹¹⁷ It appears, however, that the United Kingdom did not anticipate and address concerns raised by critics in a timely manner, vacillated in its implementation efforts, and fumbled badly on the societal acceptance issue.

2. India

The second case study of a national ID system is India. Within the last several years, India embarked on its first effort—an extremely ambitious one—to establish a national database of all citizens and distribute national identity cards to more than a billion people.¹¹⁸ Originally conceived as the multipurpose national identity card (MNIC), it was envisioned as a national register of citizens, a national register of non-citizens, and a national register of residency. India's government initiated a “pilot project” to introduce the MNIC in select areas of the country in 2009.¹¹⁹ The program, known as Aadhaar, or “foundation” in Hindi, began enrolling individuals in 2010 with the first Aadhaar number being issued on September 29, 2010.¹²⁰

¹¹⁴ Edgar A. Whitley, “The Identity Project: An Assessment of the UK Identity Cards Bill and Its Implications,” 2005, <http://eprints.lse.ac.uk/29117/>.

¹¹⁵ BBC, “In Full.”

¹¹⁶ Ibid.

¹¹⁷ Ibid.

¹¹⁸ Taha Mehmood, “India’s New ID Card: Fuzzy Logics, Double Meanings and Ethnic Ambiguities,” in *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, ed. Colin J Bennett and David Lyon (London; New York: Routledge, 2008).

¹¹⁹ Ibid., 114.

¹²⁰ Unique Identification Authority of India, “Aadhaar Press Release October 2012,” October 2012.

The program consists of the collection of 10 prints and iris scans of citizens, and associates them with a unique identifier into a “massive database.”¹²¹ Ultimately, 1.2 billion Indian citizens will be issued a unique identifier, a random 12-digit number, by mail. Passports, driver’s licenses, ration cards, and government health-insurance cards could either have the numbers printed on them or embedded electronically.¹²² The program captures a mix of biometric data—digital photos, fingerprints, and iris scans. The program also collects a substantial amount of biographic information to include names, addresses, genders, dates of birth, and other information, such as caste and religion. It was decided to err on the side of collecting too much versus too little information because the enrollment process was relatively lengthy and only one opportunity was really available to collect the information.¹²³

At the same time, India had embarked on a parallel effort to create a National Population Register while issuing the identity cards, or MNICs, to the citizens of India. The Group of Ministers (GoM) determined that the efforts should fall within a new entity, the Unique Identification Authority of India (UIDAI), within the Planning Commission. According to the UIDAI, as of June 2013, over 360 million enrollments in the Aadhaar had been completed, and India was predicted to be on track to complete 600 million enrollments by 2014.¹²⁴

Several factors motivated the effort to establish India’s national identity program. Those factors included enhancing security, gaining efficiencies in benefit distribution, and enhancing economic opportunities for people lacking access financial systems. The initial impetus for the pilot was the recommendation of the GoM that had been formed in 2000 on the recommendation of the Kargil Review Committee. The committee’s purpose was to study the causes of the Kargil War between Pakistan and India, which for India,

¹²¹ Amol Sharma, “India Launches Project to ID 1.2 Billion People,” *Wall Street Journal*, sec. Technology, September 29, 2010, <http://online.wsj.com/article/SB10001424052748704652104575493490951809322.html>.

¹²² Ibid.

¹²³ Ibid.

¹²⁴ Unique Identity Authority of India, “APNA AADHAAR,” June 2013, at p. 6. (the monthly newsletter describes the number of enrollments as over 36 “crore.” Crore is the Indian term for 10 million, thus 36 crore is the equivalent of 360 million.

was a “big event” similar to 9/11 in the United States.¹²⁵ One proposal was to take steps to issue ID cards to border villagers in certain vulnerable areas on a priority basis. The Indian government set up a pilot project in 2003 for the introduction of the MNIC in select districts.¹²⁶

In addition to the security related concerns, India has also been motivated by reasons related to economic development, and the efficient and secure distribution of benefits. According to the *Wall Street Journal*’s treatment of the issue.

The country’s leaders are pinning their hopes on the program to solve development problems that have persisted despite fast economic growth. They say unique ID numbers will help ensure that government welfare spending reaches the right people, and will allow hundreds of millions of poor Indians to access services like banking for the first time. The Indian government is expected to spend as much as \$250 billion over five years on programs aimed at the poor, including subsidies for food, diesel, fertilizer and jobs. But 40% of the benefits, as the system now stands, will go to the wrong people or to “ghosts” with fake identification papers, according to a report by brokerage firm CLSA Asia-Pacific Markets. Today’s ration cards, for example, are issued on paper, and are relatively easy to forge or doctor.¹²⁷

The effort is acknowledged to have a role in reducing fraud, but India has emphasized its role in economic development, noting that it has the potential to bring into the financial system the roughly two-thirds of Indian adults who do not have bank accounts.¹²⁸ Leaders of the effort believe that it can help the poor, who often have few or no documents to prove who they are or where they live. “You have a whole mass of people who are shut out of society. A lack of identity is a big source of exclusion. You’re giving them a key to social services.”¹²⁹

India’s efforts were facilitated to a large degree by a unique partnership between the government and a group of successful Indian entrepreneurs who, in a sense, applied

¹²⁵ Mehmood, “India’s New ID Card,” 114.

¹²⁶ Ibid.

¹²⁷ Sharma, “India Launches Project to ID 1.2 Billion People.”

¹²⁸ Ibid.

¹²⁹ Ibid.

their tech savvy to launch a type of national service project. To lead the project, India's former Prime Minister selected Nandan Nilekani, formerly CEO of Infosys Technologies Ltd., who had helped pioneer offshore technology services. Nilekani, in turn, recruited fellow Indians with ties to the global technology industry, and asked tech companies, such as Intel, Google, Oracle Corp., and Yahoo, in November 2009, "to send Indian-origin engineers to contribute to the cause, either on paid sabbatical or as volunteers. More than 20 people joined the effort."¹³⁰

Several have leveled criticisms of the Aadhaar system, with some asserting that in India, individuals can prove their identities in a multitude of ways and that having so many options has made establishing their identity confusing. Critics note that the reliability of Aadhaar to establish a citizen's identity is under a cloud as the card itself is not necessarily proof of citizenship.¹³¹ People who are not themselves citizens can obtain the card as it is compulsory to access various programs, such as obtaining driver's licenses, opening bank accounts, and obtaining certificates related to birth, death, marriage, property registration, domicile, and income certificates.¹³²

Due to the broad range of transactions to which Aadhaar will be tied, critics also contend that it is not a voluntary system as the government has asserted. They note that while signing up is technically voluntary, any government agency or company will be allowed to require a unique ID as proof of identity. Critics assert, therefore, that it amounts to a de facto mandate for people to enroll.¹³³ They also express concern that it could be used by businesses or the government to discriminate against individuals in the provision of services provided, and also note that it could also be a huge source for data

¹³⁰ Sharma, "India Launches Project to ID 1.2 Billion People."

¹³¹ Mail Online, "India's Identity Crisis: Between Aadhaar, Passport, PAN and NPR, Why Are We Still Struggling to Prove Our Identities?," March 22, 2013, <http://www.dailymail.co.uk/indiahome/indianews/article-2297714/Indias-identity-crisis-Between-Aadhaar-passport-PAN-NPR-struggling-prove-identities.html>.

¹³² Neha Pushkarna, "India's Identity Crisis: Between Aadhaar, Passport, PAN and NPR, Why Are We Still Struggling to Prove Our Identities? Capital Hopes to Do Everything with Aadhaar," *Mail Online*, March 22, 2013, <http://www.dailymail.co.uk/indiahome/indianews/article-2297714/Indias-identity-crisis-Between-Aadhaar-passport-PAN-NPR-struggling-prove-identities.html>.

¹³³ Sharma, "India Launches Project to ID 1.2 Billion People."

mining.¹³⁴ Yet, many of the people for whom it would seem that obtaining such document would be most difficult, express the benefits of the system related to the efficient and secure distribution of goods and services. It is hoped that the IDs would keep people from cheating the welfare system and obtaining food rations for which they do not qualify. “It will take fraud out of the government schemes,” said Mr. Anjaiah, a citizen who relies on subsidies to feed his family. “Then it will be guaranteed I get what I deserve.”¹³⁵

One issue that does not seem to be of concern with the program is the ability of the system to establish one-to-one correspondence accurately between real people and electronic identities on the CIDR (central ID repository). The government embarked on a proof of concept trial in 2010, and study of efficacy of the system after the enrollment of 84 million residents. The fact that both fingerprints and irises were being captured appeared to significantly increase the levels of accuracy in enrolling residents.¹³⁶

3. South Africa

In 1997, the government of South Africa, through its Department of Home Affairs awarded a contract for the development of an Automated Fingerprint Identification System (AFIS) database, which would then be combined with the country’s population register, followed by the issuance of identity cards to the entire population.¹³⁷ South Africa’s national ID system was known as the Home Affairs National Identification System (HANIS). Yet, it is only very recently, since the summer of 2013, that these efforts, which are anchored by a Smart ID system, have been rolled out.¹³⁸ Although

¹³⁴ Sharma, “India Launches Project to ID 1.2 Billion People.”

¹³⁵ Ibid.

¹³⁶ Hardeep Guide Singh, “Role of Biometric Technology in AADHAR Enrollment,” January 21, 2012, <http://dspace.thapar.edu:8080/dspace/handle/10266/1734>.

¹³⁷ Breckenridge, “The Elusive Panopticon,” 39.

¹³⁸ Marine Jacobs, “Smart ID Card Rollout Underway,” *DefenceWeb*, August 26, 2013, http://www.defenceweb.co.za/index.php?option=com_content/0/00 0:00 AM&view=article&id=31673:smart-id-card-rollout-underway&catid=54:Governance&Itemid=118.

certain elements of the HANIS system had been previously been implemented, commenters have described the delays surrounding its implementation as a “debacle.”¹³⁹

South Africa embarked on its national identity card system as a result of national security concerns within South Africa in the 1980s.¹⁴⁰ The government of P. W. Botha decided, in 1981, to issue a “single, fingerprint authenticated, identity document to all South Africans, white as well as black.”¹⁴¹ This decision stemmed from conflicts with the African National Congress that had staged attacks on oil refineries.¹⁴² With the military and certain government elements believing that South Africa was facing a Soviet inspired “Total Onslaught,” the national fingerprint register of all “white, Indian, and coloured South Africans” was a key element of the government’s strategy including its professed need to enhance the sophistication of identity documents.¹⁴³ Over time, the justifications for the continuation of the identity system evolved to encompass things like ““orderly public administration; for business or for identifying dead bodies,”” yet the objective of completing a national registration remained.¹⁴⁴ Another driving force behind the HANIS project involved the intense discussions surrounding South Africa’s post-Apartheid welfare system with “the first meaningful” discussions taking place in 1994 related to the first social and economic policy. A need existed to distribute benefits to millions of poor South Africans, and do so in a way that was fair and identified only eligible South African recipients.¹⁴⁵ The solution that emerged was to adopt an automated fingerprint identification system and an identity card.¹⁴⁶ The current justification for the issuance of the Smart ID card is to address the issue of identity fraud.¹⁴⁷

¹³⁹ Breckenridge, “The Elusive Panopticon.”

¹⁴⁰ Ibid., 41.

¹⁴¹ Ibid.

¹⁴² Ibid., 41–42.

¹⁴³ Ibid., 42.

¹⁴⁴ Ibid.

¹⁴⁵ Ibid.

¹⁴⁶ Ibid.

¹⁴⁷ Jacobs, “Smart ID Card Rollout Underway.”

One characteristic of South Africa's system that received attention in press reports during the UK's consideration of a national identity card is that only South Africa's system combined smart card applications and identification technologies.¹⁴⁸ It was held up as "an excellent example of the use of biometrics for purely civilian and humanitarian ends."¹⁴⁹ The South African model, unique in its combination of elements of photographic identification, biometric registration, and smart card applications, has been seen as an example worth examining more closely and possibly emulating.¹⁵⁰ The current effort has the identification cards being issued free of charge to 16-year-old youth who are first time applicants.¹⁵¹

Among the issues that have resulted in strong criticism, and controversy, was the procurement of the HANIS technology, and how the government handled that issue. Allegations of favoritism were raised in the awarding of contracts and critics have questioned the government's decision to pursue smart-trip technology, as opposed to the then standard bar-code technology, given that at the time smart-trip technology was not dramatically more secure than bar-code technology.¹⁵² The decision to adopt smart-card technology resulted in the government making plans to use the card to host all key functions of government information processing relative to individuals; thus, making the card the "lynch-pin of a host of bureaucratic and commercial functions."¹⁵³

The problem for South Africa as it sought to find the technical solution to implement its proposal was "the same issue that had bedeviled fingerprint classification and storage in general, and the construction of a centralized registries in particular, since the turn of the twentieth century: no uncontested standard existed for smart card

¹⁴⁸ Breckenridge, "The Elusive Panopticon," 40.

¹⁴⁹ Ibid.

¹⁵⁰ Colin J. Bennett and David Lyon, *Playing The Identity Card: Surveillance, Security and Identification in Global Perspective* (New York: Routledge, 2008), 40, <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=529287>.

¹⁵¹ Jacobs, "Smart ID Card Rollout Underway."

¹⁵² Breckenridge, "The Elusive Panopticon," 42.

¹⁵³ Ibid., 45.

fingerprint identification, either in South Africa or internationally.”¹⁵⁴ In other words, until an international standard was developed, manufacturers were promoting their own systems as the “ultimate solution.”¹⁵⁵ In turn, a lack of standardization resulted, which critics contend leads to significant error rates.¹⁵⁶

Some say that South Africa’s implementation issues proved challenging precisely because the country had been such a rapid adopter of fingerprinting as a means of identification. Over the years, South Africa has adopted at least five separate nationwide systems adopted by different departments of the government independent of Home Affairs, to include police; social welfare, drivers’ licensing, and the courts and prisons.¹⁵⁷ This system created issues of compatibility, and large differences between the electronic storage required to retain the original fingerprint and its “mathematical template.” The reality initially encountered by the government was the fact that the smart cards have very limited capacity with budgetary constraints of large-scale identification projects forcing the adoption of the cheapest and the smallest cards.¹⁵⁸ However, according to more current reports, the Smart ID cards are now equipped with microchips that contain the biographic information on the holder, and also contain the fingerprint image that allows the verification of identity by scanning the individual’s fingerprint and comparing it against the one contained on the card.¹⁵⁹

South Africa’s identification system evolved from being one intended to address security and control of the population, to become a key element in the efficient administration of public services. South Africa’s national ID system, while extremely delayed in its roll out, is widely recognized as one that combined smart card technology with unique biometric identifiers. Its rapid adoption of technology and the absence of

¹⁵⁴ Breckenridge, “The Elusive Panopticon,” 47.

¹⁵⁵ Ibid.

¹⁵⁶ Ibid., 51.

¹⁵⁷ Ibid., 47.

¹⁵⁸ Ibid.

¹⁵⁹ Jacobs, “Smart ID Card Rollout Underway.”

standards, however, made it vulnerable to the dictates of vendors and resulted in a lack of standardization and duplicate systems.

4. Germany

Germany is known for having a long history of registering and identifying its citizens, which began in 1876 when the government took over the function of registering births, deaths, and marriages; a function previously performed by the churches.¹⁶⁰ National identity cards have had several iterations over the years beginning with their use during the Third Reich when the cards came into existence based on a law passed in 1937, and served as proof of identity and citizenship.¹⁶¹ The cards captured fingerprints, which became mandatory for conscripts and the Jewish population.¹⁶² The identity card became mandatory for all persons age 15 and older starting in 1939.¹⁶³ Subsequently, with the advent of World War II, citizens and persons in occupied territories were registered, and registration was most notoriously used to register Jewish citizens and in connection with facilitating their deportations, and with the administration of concentration camps.¹⁶⁴

Under German law, citizens must possess either a passport or an identification card. However, concerns over the use of a unique identifier in Germany, given its history, have led to the Federal Constitutional Court banning the use of the unique identifier for census purposes, as well as by the Federal Parliament. Although the German ID card has a unique registered number, it may not be used for any administrative purpose other than criminal or investigative purposes.¹⁶⁵ Nevertheless, Germany has also introduced a

¹⁶⁰ Torsten Noack and Herbert Kubicek, “The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany,” *Identity in the Information Society* 3, no. 1 (March 25, 2010): 87–110, doi:10.1007/s12394-010-0051-1.

¹⁶¹ *Ibid.*, 93.

¹⁶² *Ibid.*, 88.

¹⁶³ *Ibid.*, 93.

¹⁶⁴ *Ibid.*, 88.

¹⁶⁵ Noack and Kubicek, “The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany.”

unique tax identification number, but its use is considered to be “sector specific.”¹⁶⁶ The administration of the registration of citizens occurs at local municipality level, and until 2006, had been regulated at the state level under a national framework document, and efforts had been made by some states to establish state level centralized registers. At that time, the legislative authority was transferred exclusively to the national level. Debate continues in Germany over the degree of desirable centralization.¹⁶⁷

Germany has moved to an electronic machine-readable ID card, with legislation enacted in 1987, governing its provisions.¹⁶⁸ Germany’s new eID card, introduced for the purpose of facilitating online authentication, is smaller than the previous card, although for ease of use, and at the request of law enforcement officials, the photograph and type size were maintained. In addition, the card was equipped with radio frequency identification (RFID) technology to maintain conformity with Germany’s electronic passport; thus, both the ID card and the e-passport allow for the storage of biometric features, i.e., face photo, and fingerprints.¹⁶⁹ The existence of the RFID technology allows the card to perform three functions: authentication, travel control, and e-signature; the authentication and e-signature features are opt-in features at the users’ discretion.¹⁷⁰

It is the view of this author that that REAL ID does not constitute a national ID system. Although some may resort to scare mongering on this issue just simply because they are opposed to government regulation in the area of identity documents, many people have genuine concerns, and fear, that REAL ID could be a significant step on the way toward a national ID. Therefore, the example of Germany, which the world recognizes as epitomizing the dangers of a national ID system under the control of a government bent on the oppression and commission of genocide against members of its population, bears examination for the caution with which it has approached the issue and sought to address concerns about the risks to individuals related to such a system.

¹⁶⁶ Noack and Kubicek, “The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany.”

¹⁶⁷ Ibid.

¹⁶⁸ Ibid., 95.

¹⁶⁹ Ibid., 96.

¹⁷⁰ Ibid.

One thing that the German government has done is give individuals some degree of control as to how the card would be used by the individuals and by others. For example, one of the principal purposes of the eID was to allow the use of digital signatures, and the facilitation of authentication of interactions between individuals, and business and government entities to help modernize public administrations and strengthen internal security. This gave greater assurance to business, and in turn, allowed individuals to have greater access to ebusiness applications.¹⁷¹ An example of granting of individual control to individuals is that in Germany, the eID could also serve as a travel document within the European Union (EU). Thus, German citizens could choose to use their e-passport for travel purposes, or use their e-ID for the same purpose. The requirement, however, was that the eID, if used as a travel document, would need to have the fingerprints embedded in the document. The Germans determined that they could allow individual citizens to decide whether they wanted to provide the fingerprints so that the card could embed that information into the card, and thus, facilitating its use as a travel document. Alternatively, the citizen could choose not to include the fingerprints, in which case, the e-ID could not be used for travel, and instead, the citizen would need to use the traditional e-passport. In addition, the government enlisted the assistance of service providers, and used them to test the electronic identification proof of the eID card so that the cards functioned as intended when unveiled in 2010.¹⁷²

C. CHAPTER RECOMMENDATIONS AND CONCLUSIONS: IMPLICATIONS FOR THE IMPLEMENTATION OF REAL ID

A number of takeaways and lessons learned from this comparison might have implications for the U.S.' implementation of REAL ID and its efforts to gain societal acceptance of the effort by addressing concerns that REAL ID constitutes a national ID system. This issue will especially be important as DHS begins to enforce REAL ID and impose consequences on holders of non-compliant driver's license and identification documents. Such efforts, in turn, will renew opposition to REAL ID and renew possible

¹⁷¹ Noack and Kubicek, "The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany," 89.

¹⁷² Ibid., 93.

challenges, legal, and otherwise, to its requirements. With that in mind, DHS would do well to adopt some lessons from the comparison countries.

Get Out ahead of the Critics: (UK)

Considerable opposition will be mounted against efforts to improve security when they impact individuals and by restricting them or imposing additional burdens. DHS must clearly communicate its message, educate the general public and the states, and address the challenges mounted by critics to ensure the public understands REAL IDs objectives and how the government has and will continue to respond to concerns.

Proceed with Caution before Pursuing Anything Like an Identity Register: (UK)

While not applicable to the REAL ID in its current form, one of the most controversial aspects of the most recent UK effort on a national ID system was the maintenance of a national register that would collect information on the entire population in a centralized manner. While not unusual in national ID systems, its existence proved particularly controversial and confusion and misinformation occurred as to whether REAL ID establishes a similar system. That misinformation needs to be confronted directly and firmly, while addressing why it is critical that states share information regarding applicants for driver's licenses and identification documents.

Enlist the Business Community, Particularly the Technology Sector, in Furtherance of the Effort: (India)

This issue is particularly important when implementing complex systems that depend upon non-government systems and systems dealing with technology and implementation and adoption issues. Recent developments regarding surveillance activities of the National Security Agency (NSA) have eroded the trust between business and government on issues affecting individual privacy. However, DHS should enlist private entities in advising as to the best way to develop tools at both the federal and local level to help states effectively implement REAL ID in a secure and reliable manner.

Set Standards for the Technology: (South Africa)

As biometrically enabled ID cards need to distinguish between individuals presenting them to ascertain that the individual presenting the document is actually the individual to whom the card was issued, reliable technology is necessary to match the card quickly and accurately to the presenter, and is important for the system to be usable and accurate. Part of the implementation challenges for South Africa and others has been that the technology supporting the identity management and verification efforts was not standardized, and as a result, various incompatible systems were established that would not effectively interact with each other.

Beware of Feeding the Beast of Business Interests: (South Africa)

While the federal and state governments may do well to enlist the assistance of business, and will always be dependent upon its products and services to implement any effective government technology based program, let alone a national ID system, the management of how business supports critical government functions must be monitored to ensure that the government does not promote the spread of systems supporting incompatible and interoperable government functions. The government must also take care to ensure that business does not become itself too powerful in making use of that information about individuals in ways that could be seen by the public as threatening information security and individual privacy.

Address Concerns Regarding the Accuracy of the System by Encouraging the Capture of Multiple Biometrics: (India)

India found itself faced with the enrollment of an enormous population. The accuracy of the enrollment and of the matching of identity card to enrollees was legitimate concern and was critical to address for the system to be reliable and perform its intended purpose. India chose to collect more than one form of biometrics, to include fingerprints and iris scans. Proof of concept and post enrollment studies have reinforced the wisdom of that decision and have served to increase overall confidence in the accuracy of the system. The federal government should encourage the use of multiple

biometrics, as well as to ensure that confidence in the system's accuracy grows and inaccuracies do not become a reason to oppose the system.

Give People Choices Regarding the Use of Their Personal Information (Germany)

Germany successfully implemented a national identity card notwithstanding its history and legitimate concerns of using identity documents to oppress its citizens. It has been careful to provide choices to the population regarding how much information it provides and how that information will be used. Giving citizens control over their information diminishes the ability of the government to abuse the identity cards, while empowering the citizens to make judgments about how much private information they want to provide for additional convenience.

D. CONCLUSION

The REAL ID Act has provided the United States the opportunity to enhance the security and reliability of state driver's licenses and identity documents through the issuance of federal standards by DHS governing the issuance of those documents. Since the introduction of the legislation in Congress, critics have raised concerns that the program was establishing a national ID as part of a coercive identity regime. While the federal government continues to assert that REAL ID does not constitute a national ID scheme, this issue has been one contributing factor in the reluctance of many states to come into full compliance, thus weakening the efforts to address this vulnerability on a national basis. This chapter has sought to explain the claim that REAL ID is a national ID, the U.S. response to the claim, and shows how US. efforts differ from those of countries that have established or have sought to establish a national ID system.

As DHS addresses the lingering concerns, and adopts measures to promote full implementation by the states, it would do well to study and learn from the experiences of the other countries. Doing so will allow it to undertake public messaging to distinguish the U.S. efforts from those of countries with national ID systems and help to promote societal acceptance. DHS and the states must engage with each other to ensure smart and effective implementation of the law to minimize the effects on privacy and security of the

information. DHS should also explore how best to fund, and allocate grants to the states to facilitate the acquisition of technical support. Technology investments and acquisitions should support verification activities in a manner that is integrated, and serves national security interests that protect privacy and information security.

IV. PRIVACY ISSUES ASSOCIATED WITH REAL ID

As discussed earlier, deficiencies in the security of the issuance process related to state driver's licenses and identification documents had enabled the hijackers to remain in the United States and access the air transportation system, raising concerns about the integrity of the issuance process. This situation led to the 9/11 Commission's recommendations regarding the need for federal standards for the issuance of birth certificates and other sources of identification, such as driver's licenses and state identification cards.¹⁷³ As part of the federal efforts to set and implement such standards, DHS has required states to utilize technology to embed data in the MRZ of the identification documents.¹⁷⁴ The MRZ refers to a specific physical area on the document or card where data is encoded in a machine-readable format.¹⁷⁵ It allows the data appearing on the face of state-issued driver's licenses and identification documents to be verified in real-time. This chapter addresses the following: the required data elements for REAL ID documents, the technology specified for the required MRZ (specified as 2D Barcode technology), how it compares to RFID technology—the most likely alternative to 2D Barcode technology, and the process through which DHS selected this technology and addressed privacy related concerns regarding its use.

REAL ID requires state driver's licenses and identity documents to include defined data elements and make them accessible through a common machine-readable technology. The use of machine-readable identity cards has increased significantly to allow the efficient transition from a manual to an automated authentication process.¹⁷⁶ The text information and biometric identifiers, such as facial image, signature, fingerprint

¹⁷³ National Commission on Terrorist Attacks upon the United States, *9/11 and Terrorist Travel*. (Vulnerabilities include the submission of false documents to demonstrate residency, use by an imposter of documents relating to another individual, and tampering with legitimate documents to enable their use to demonstrate eligibility for state documents.)

¹⁷⁴ 6 C.F.R. § 37.19.

¹⁷⁵ National Commission on Terrorist Attacks upon the United States, *9/11 and Terrorist Travel*, 13, 44.

¹⁷⁶ Afzel Noore, Nikhil Tungala, and Max M. Houck, "Embedding Biometric Identifiers in 2D Barcodes for Improved Security," *Computers and Security* 23, no. 8 (December 2004).

template, or iris template, are typically stored on the card and enable verification of the identity of the owner. The technical standards for the machine-readable technologies to be employed by the states are set forth at 6 C.F.R. § 37.19.¹⁷⁷ For purposes of this discussion, it is sufficient to know that DHS established the Portable Data File 417 barcode (PDF417) as the required technology to embed data into the MRZ.

A. THE 2D BARCODE

The PDF 417 is a type of 2D “stacked” barcode technology able to encode over 1 kilobyte of data.¹⁷⁸ Figure 1 shows an image of a 2D barcode.

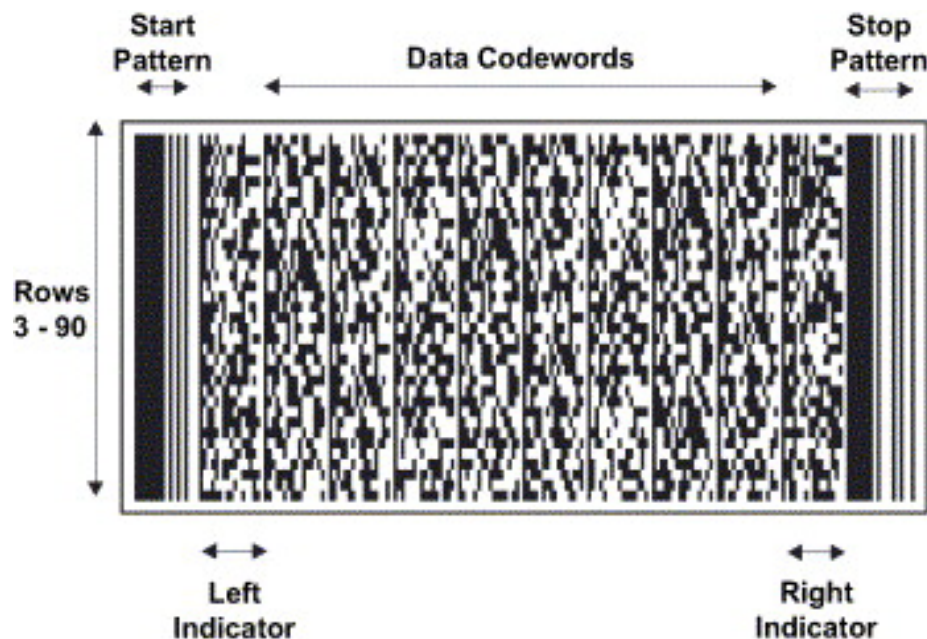


Figure 1. PDF 417 2D Stacked Barcode¹⁷⁹

¹⁷⁷ The standard specified is ISO/IEC 15438:2006(E) Information Technology—Automatic identification and data capture techniques—PDF417 symbology specification.

¹⁷⁸ Brendon Bass, “What Is an PDF417 Barcode,” *Am Labels*, December 15, 2010, <http://www.support-amlablabels.co.uk/2010/11/what-is-an-pdf417-barcode>.

¹⁷⁹ “PDF 417 2D Stacked Barcode,” accessed March 4, 2013, https://www.google.com/search?q=PDF+417&rlz=1C1CHMO_enUS580US580&espv=210&tbm=isch&tbo=u&source=univ&sa=X&ei=zE4tU_j9E8na2QWDh4HwDw&ved=0CD0Q7Ak&biw=1024&bih=724#q=google+images+PDF+417+2D+Stacked+Barcode&tbm=isch.

Recently, 2D barcodes with extended data capacity have been used to store information on ID cards compactly. According to one site, this barcode technology allows over 100 times more data to be stored as compared to traditional one dimensional, linear barcodes. Popular applications of this barcode technology include “mailing, logistics and inventory management.”¹⁸⁰ The information can be stored securely and inexpensively and its advantages include the fact that information can be read from the labels using a “slightly modified handheld laser or linear CCD scanners.”¹⁸¹

The PDF417 2D barcode is widely adopted by major industries and various national and international standards and industry organizations, such as the American National Standards Institute (ANSI), the International Civil Aviation Organization (ICAO), and the Association for Automatic Identification and Mobility (AIM), because of its extended data capacity and error correction capabilities.¹⁸² The correction code capability allows the information on the barcode to be read even when the barcode has been partially lost or destroyed.¹⁸³

According to one source, the PDF technology has become the preferred means of coding ID information inexpensively and with the capacity for a large amount of data.¹⁸⁴ The PDF approach is valuable in situations in which the database is not accessible at the point that the item will be read.¹⁸⁵ Another advantage is the capability to store biometric data files, such as photographs, fingerprints, and signatures.¹⁸⁶

The REAL ID Act specified what minimum elements needed to be contained on the face of the cards, but it did not specify what data needed to be stored in the MRZ.¹⁸⁷

¹⁸⁰ “PDF 417 2D Stacked Barcode.”

¹⁸¹ Ibid.

¹⁸² Ibid. (citing AIM, 1994).

¹⁸³ Ibid.

¹⁸⁴ Ibid.

¹⁸⁵ Easesoft.net. “PDF417 Symbology,” February 24, 2013, <http://www.easesoft.net/PDF417.html>. (The PDF approach capability is consistent with the situation with REAL ID documents where, likewise, the database will not be accessible at the point at which the documents will be read, e.g., the TSA screening station, the federal building, or the nuclear facility.)

¹⁸⁶ Ibid.

¹⁸⁷ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*,” 10.

However, the regulation specifies that PDF417 bar code standard must encode the following defined minimum data elements, seen as necessary for DMVs and law enforcement, within the state documents.

- Expiration date
- Full legal name, unless the state permits an applicant to establish a name other than the name that appears on a source document, pursuant to § 37.11(c)(2)
- Date of transaction
- Date of birth
- Gender
- Address as listed on the card pursuant to § 37.17(f)
- Unique driver's license or identification card number
- Card design revision date, indicating the most recent change or modification to the visible format of the driver's license or identification card
- Inventory control number of the physical document
- State or territory of issuance¹⁸⁸

B. THE RULEMAKING PROCESS AND CONSIDERATION OF RFID AS A POSSIBLE ALTERNATIVE TECHNOLOGY

DHS discussed the technology it would require for REAL ID purposes through the rulemaking process. DHS explained why it was requiring states to use the PDF 417 2D barcode and also addressed why another technology considered, RFID, was not suitable for REAL ID purposes. The explanation was offered in the context of the PIA related to the rulemaking process.

Under the Homeland Security Act of 2002, DHS is required to have the DHS Chief Privacy Officer conduct a “privacy impact assessment of proposed rules of the Department.”¹⁸⁹ In addition, pursuant to the e-Government Act of 2002, a PIA is required whenever federal agencies seek to develop or procure information technology that

¹⁸⁸ Department of Homeland Security, *Final Rule*.

¹⁸⁹ *The Homeland Security Act of 2002*, Public Law 107–296 (November 25, 2002).

collects, maintains, or disseminates identifiable information.¹⁹⁰ The Department of Homeland Security issued its PIA for the REAL ID final rule on January 11, 2008.¹⁹¹ That PIA which was issued in advance of the Final Rule issued later that month, addressed the privacy implications of various aspects of the REAL ID rule raised by commenters during the NPRM. The PIA assessed five major privacy areas associated with the REAL ID Act and the proposed rule. The privacy area relevant to this discussion deals with the technology required by the REAL ID requirements. The issue was whether and how the information stored in the machine-readable zone (MRZ) on the cards will be protected from unauthorized use.¹⁹²

Among the issues addressed was the suggestion by commenters that DHS limit data elements to be included in the MRZ, and recommending instead, that the MRZ include only a pointer to a database where the information could be found and accessed only by law enforcement.¹⁹³ DHS responded that while a pointer system might seem preferable, it would require a centralized national database to allow law enforcement from all jurisdictions to access the information, and furthermore, law enforcement would need access to technology to make such database information available on a mobile basis—something that not all law enforcement entities had the capability to access.¹⁹⁴ It did, however, determine that while it would maintain the requirement to include the data elements in the MRZ, it would eliminate the name history as one of the required data elements.¹⁹⁵

¹⁹⁰ *E-Government Act of 2002*, Public Law 107–347, 2002, http://books.google.com/books?hl=en&lr=&id=6_3qiQtH9woC&oi=fnd&pg=PA1&dq=%22511.+Findings+and%22+%22Findings.--Congress+finds+the%22+%22Most+Internet-based+services+of+the+Federal%22+%22performance+and+outcomes+within+and+across%22+%22Purposes.--The+purposes+of+this+Act+are+the%22+&ots=XbsGq-1EQy&sig=h0rfGpGwK_MkZL8hewfT2z2CRro.

¹⁹¹ Department of Homeland Security, *Final Rule: Privacy Impact Assessment*, January 11, 2008.

¹⁹² *Ibid.*, 3.

¹⁹³ *Ibid.*, 10.

¹⁹⁴ *Ibid.*, 14.

¹⁹⁵ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*, 10.

C. PROTECTION OF PII IN THE MRZ

The PIA related to the NPRM clearly states that nothing in REAL ID required DHS to promulgate regulations setting federal standards for the protection of the privacy of individuals who apply for and receive driver's licenses or state identification cards.¹⁹⁶ Nevertheless, the Chief Privacy Officer, through the PIA, noted that several references in the legislative history indicated that Congress intended for protection to be afforded.¹⁹⁷ The PIA noted that Congress expected this issue with respect to information contained in the MRZ, citing the following language from the Conference Report:

There has been little research on methods to secure the privacy of the data contained on the machine-readable strip. Improvements in the machine readable technology would allow for less data being present on the face of the card in the future, with other data stored securely and only able to be read by law enforcement official.¹⁹⁸

According to the Chief Privacy Officer, this statement suggests that Congress wanted to secure the privacy of the data contained on the MRZ of the credential, and make it accessible only to law enforcement officials.

DHS considered the findings of the Chief Privacy Officer, but determined that REAL ID does not authorize DHS to limit third-party private sector uses of the information appearing in the front of the REAL ID document or in the MRZ. It further recognized that the 2D Barcode might have vulnerabilities and technology limitations compared to other available technologies. It explained that it nevertheless selected the 2D Barcode because it was already in use by 45 jurisdictions and law enforcement across the country, and making a different technology choice could hamper law enforcement and prove to be an additional financial burden on the states. Instead, DHS emphasized that states could take action, through their own laws, to limit third-party use, citing the example of California, Nebraska, New Hampshire, and Texas, which had taken action to

¹⁹⁶ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act: In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 3–4.

¹⁹⁷ *Ibid.*, 5.

¹⁹⁸ *Ibid.*, 4. (citing H.R. Rep. No 109–72 (2005) (Conf. Rep.).

limit third-party use of the MRZ.¹⁹⁹ It further noted that the AAMVA had issued a model act limiting such use. That model legislation authorized the use of 2d bar code scanners by third-party users only for the limited purposes of age verification.²⁰⁰

The PIA notes that the DHS Privacy Officer had “urged DHS to adopt encryption to protect PII on the MRZ from skimming by third parties other than law enforcement or DMVs.”²⁰¹ Nevertheless, the NPRM PIA noted that to encrypt the data to prevent unauthorized third party access, it would be necessary to establish a cryptographic key to decrypt, and to provide that key to permitted parties to access the information. “The need for a key infrastructure to support access to encrypted 2D bar code data raises an important challenge for implementation of encryption.”²⁰²

The NPRM had asked for public comment on the issues of: 1) whether implementing encryption was feasible from an operational and cost perspective, and 2) whether encryption could be deployed in a manner that would ensure access to the information by law enforcement.²⁰³ The PIA noted it was recognized that to implement encryption, it would be necessary to establish a “complex and comprehensive” exchange of encryption keys among all 56 jurisdictions involved in issuing and accessing REAL ID driver’s licenses and identification cards.²⁰⁴ Footnote 50 of the NPRM PIA describes the complexity as follows.

With 2D bar codes, a symmetric cryptographic key system would need to be implemented. With a symmetric system, a multi-key or single key implementation could be used. In a multi-key implementation, although a larger the number of keys creates a more secure system, because a single key compromise does not compromise the entire system, this large number

¹⁹⁹ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act: In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 4. (citing H.R. Rep. No 109–72 (2005) (Conf. Rep.).

²⁰⁰ Ibid.

²⁰¹ Ibid.

²⁰² Department of Homeland Security, *Notice of Proposed Rulemaking: Privacy Impact Assessment*, March 1, 2007, 16.

²⁰³ Ibid.

²⁰⁴ Ibid.

of cryptographic keys would need to be accessible to the law enforcement personnel wherever they would be reading the driver's license. A single key implementation would avoid the complexities of needing a key infrastructure, but this greatly increases the risk that this single key could be compromised. Although employing a single key greatly simplifies the procedure to make available the cryptographic key to law enforcement personnel, the compromise of this single cryptographic key would compromise all driver's licenses created with it. In this case, encryption could create a false sense of security if a license holder thought his or her information was truly secure and it was not, because an unauthorized third party compromised the key. Not only do these implementation operations present operational and security risks, they also factor into the privacy risks with the selection of an implementation.²⁰⁵

The NPRM PIA noted that under principles of data minimization protections, if encryption were to be used, then the MRZ should have fewer data elements and more limited personal information, especially the credential holder's address.²⁰⁶

Many comments were received both for and against encryption. DHS acknowledged that the potential to skim PII from the MRZ raises important privacy concerns, but it struck the balance in favor of the need for law enforcement to have easy access to the information, as well as complexities and costs of implementing an encryption infrastructure.²⁰⁷ Thus, DHS did not require encryption "at this time." It noted, however, "if the States collectively determine that it is feasible to introduce encryption in the future, DHS will consider such an effort, so long as the encryption program enables law enforcement easy access to the information in the MRZ." The PIA that accompanied the final rule indicates that DHS supports efforts to find technological improvements to protect the personal information on the MRZ, as well as state efforts to limit skimming of personal information from the cards.²⁰⁸

²⁰⁵ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act: In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 4.

²⁰⁶ *Ibid.*, 17.

²⁰⁷ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Final Rule*, 14–15.

²⁰⁸ *Ibid.*, 15.

Among those dissatisfied with the DHS response regarding how it sought to protect the personal information on the cards, was EPIC, which was among the commenters urging DHS to adopt encryption as a means of protecting information stored on the MRZ. In its report on REAL ID's implementation issued in May 2008, EPIC expressed its disagreement with DHS' decision to leave the information on the cards unencrypted. It noted that DHS did so notwithstanding the recommendations of "independent privacy and security experts and the agency's own Privacy Office," and thereby, created unnecessary security risks to individual privacy.²⁰⁹ EPIC's report cited examples of cases in which unencrypted information had been accessed by unauthorized users, and indicated that while it anticipated DHS' responses regarding the difficulties with the use of encryption.²¹⁰ It criticized DHS for failing to consider an alternative that EPIC had proposed, which was to not enter any personal information onto the MRZ, but instead, embed a unique identifier into the MRZ, which would "point" to the records in a national database. Those records, in turn, would only be accessible via the use of a password or encryption.²¹¹ However, as DHS had noted in its responses to comments, such an approach would suggest the need for a national database, which DHS did not want to establish given concerns about creating a national registry or national ID.

In addition to EPIC, the New York American Civil Liberties Union (NYCLU), has also been a vocal opponent of storing information in the MRZ, and raised concerns beyond those raised by EPIC. In its 2009 report setting forth its opposition to REAL ID, the NYCLU raised a wide-ranging, but arguably unsupported criticism, of the use of the MRZs on privacy grounds, including: 1) the MRZ makes the information readily accessible and able to be used by thousands of state and local officials, as well as private entities to easily track individuals; 2) the failure to encrypt the information allows anyone with a reader to access the information; 3) the unencrypted information contained in the databases and the MRZ is a treasure trove for identity thieves creating one-stop shopping for access to a wide variety of documents, including SSNs; and 4) the information

²⁰⁹ EPIC: *Real ID Implementation Review*, 12.

²¹⁰ *Ibid.*, 13.

²¹¹ *Ibid.*

contained in the MRZ was of concern to labor organizations which claimed it could be used to do intrusive monitoring of workers including monitoring their trips to the restroom; and 5) the MRZ poses specific concerns for lesbian, gay, bisexual, and transgender (LGBT) individuals whose entry into clubs and purchases could be used to expose their sexuality or discriminate against them.²¹² The NYCLU's recitation of problems with the MRZ largely comes down to a concern about the absence of encryption, which DHS addressed in its rulemaking documents. It also tends to exaggerate the threat given that 2D Barcodes are unlike RFIDs that can be read from distances of a few inches, up to 20 to 30 feet away for "passive" tags, or as far away as a mile or more for some "active" tags.

D. THE RFID AS AN ALTERNATIVE TECHNOLOGY

Simultaneous with the efforts on REAL ID, DHS was seeking to implement enhanced driver's licenses (EDLs), which *did* utilize RFID technology. The EDLs were developed to address the need for cross-border travel between the United States and Canada, due to the implementation of the Western Hemisphere Travel Initiative (WHITI), which was a result of Intelligence Reform and Terrorism Prevention Act of 2004.²¹³ That legislation required that to cross the border between the United States and Canada, or between the United States and Mexico, persons seeking to do so would need to use a passport or secure documentation that established identity and status and nationality. For admission to the United States, U.S. citizens would need to establish citizenship. To accommodate this need, EDLs were developed using RFID technology. That technology allows the transmission of information electronically stored in tags in the document to be transmitted wirelessly.²¹⁴

DHS' Customs and Border Protection has adopted RFID technology to enable a number of documents to be acceptable for WHITI purposes. Among those documents are

²¹² Udi Ofer, Ari Rosmarin, and Michael Cummings, *No Freedom Without Privacy: The REAL ID Act's Assault on Americans' Everyday Life* (NY ACLU, February 2009).

²¹³ Public Law 108-458 (December 17, 2004).

²¹⁴ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act: In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*.

the U.S. Passport Card, Trusted Traveler Program cards (Global Entry, NEXUS, SENTRI and FAST), Enhanced Driver's Licenses from issuing (Michigan, New York, Vermont and Washington), New Border Crossing Card, and New Permanent Resident Card (green card).²¹⁵

Views differ as to the risks to the privacy of individuals that accompany the use of RFID technology. Some view it as a significant risk to privacy and theft of the information.²¹⁶ Others are less concerned about the risks of the technology and view it as valuable technology for secure identification purposes, while recognizing that adequate protections are necessary to ensure that PII is protected.²¹⁷ Some researchers have asserted that from a privacy protection standpoint, the RFID technology, used in items like the U.S. E-passport, poses a greater risk to privacy due to issues with skimming, eavesdropping, and other measures that result in tracking and possible identity theft.²¹⁸

Significant differences currently exist between the technology needed to support REAL ID, from that which is needed for WHITI purposes. Principally, the reason for their different uses relates to the proximity within which the information is read. In the border crossing application, the information needs to be transmitted from a distance to allow the inspectors situated at the ports of entry to view information related to that traveler at the point that the traveler approaches the inspection location. In the current situation with REAL ID documents, it is not necessary to transmit the information from a distance, because the identification documents are presented for official purposes, are in close proximity to the government official seeking to view or scan the information from the document. Nevertheless, as DHS indicated, it was open to exploring further the utility and security of the RFID technology in connection with REAL ID documents.

²¹⁵ Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act: In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*.

²¹⁶ Marci Meingast, Jennifer King, and Deirdre K. Mulligan, "Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. E-Passport," in *RFID, 2007. IEEE International Conference on RFID*, 2007, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4143504.

²¹⁷ Monica Nogueira and Noel Greis, "Uses of RFID Technology in U.S. Identification Documents," *University of North Carolina, Center for Logistics and Digital Strategy*, 2009.

²¹⁸ Meingast, King, and Mulligan, "Embedded FID and Everyday Things," 7–14.

E. ADDITIONAL PRIVACY PROTECTION MEASURES ADOPTED BY DHS

Although the proposed rule had authorized states to access each other's databases electronically, this provision was withdrawn in the final rule due to concerns raised by commenters, including states. Instead of specifically authorizing such access by states, the PIA accompanying the final rule explains that states may use existing processes to transfer information regarding a prior motor vehicle record when an individual seeks to move a license from one state to another.²¹⁹

To address concerns about including the address of certain categories of people for whom state laws authorize not disclosing that information, the final rule authorized the true address to only be maintained securely in the records of the state motor vehicle departments as opposed to being included on the face of the cards or captured in the MRZs.²²⁰

F. CONCLUSION

The events of 9/11, and the recognition of the need for more secure identification documents, resulted in a significant and controversial regulatory scheme to develop more secure state issued driver's licenses and identification documents. A key consideration in the rulemaking process was determining the technology to be used by encoding information within those documents to enable the authentication of the document. DHS considered both 2D Barcode, as well as RFID technology, and ultimately, determined that the 2D Barcode technology best suited its operational needs while reducing risk to the security of the PII, and facilitating interoperability for law enforcement purposes. As the states begin to issue REAL ID compliant documents, as technology progresses, and as additional uses for the REAL ID documents become a possibility, it will be necessary for DHS to monitor the effect of the 2D Barcode standard. It may also be the case that as technology progresses and additional security measures are developed, RFID technology may be reconsidered as the acceptable technology standard.

²¹⁹ Department of Homeland Security, "Privacy Impact Assessment for the REAL ID Final Rule," 12.

²²⁰ *Ibid.*, 10.

V. THE CLAIM THAT REAL ID VIOLATES THE TENTH AMENDMENT AND CONSTITUTES AN UNFUNDED MANDATE

This chapter focuses on the claim that REAL ID violates the Tenth Amendment and constitutes an unfunded mandate. REAL ID has come under assault by a number of states, which have resisted its implementation and label it an intrusion into state sovereignty, as well as an unfunded mandate. One of the significant impediments to the full implementation of REAL ID is that the states, through the National Governor's Association and similar entities, have asserted that REAL ID is an unfunded mandate.²²¹ It is very likely that as DHS enforcement efforts progress, states particularly opposed to REAL ID will likely engage in litigation seeking to challenge it as a violation of the Tenth Amendment. As for the claim that REAL ID constitutes an unfunded mandate, it is unclear how vulnerable REAL ID would be to any court action on that issue, but it needs to be recognized that implementation comes at considerable costs to states. The considerable expense of implementation efforts, and claims that the federal standards constitute an unfunded mandate, becomes a political rallying point that warrants attention from DHS.

As an initial matter, it is necessary to address what the Tenth Amendment prescribes, and what is commonly understood to be an unfunded mandate. The Tenth Amendment to the United States Constitution provides as follows:

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.²²²

The question for Tenth Amendment purposes is whether the federal government's actions to set standards for the issuance of driver's licenses and state identity documents constitutes sufficient interference with state powers by effectively commandeering state

²²¹ National Governors Association, National Conference of State Legislatures, and American Association of Motor Vehicle Administrators, *The REAL ID Act: National Impact Analysis*, a September 2006.

²²² U.S. Const. amend. X.

regulatory processes or functions.²²³ Alternatively, the tactic, embodied in both laws, of setting federal standards that the states must meet for the documents to be acceptable for federal purposes, as opposed to imposing direct prescriptions on the states, may sufficiently disentangle the federal government from state processes, such that the laws will survive a Tenth Amendment challenge—but it remains to be seen.

Tenth Amendment principles have particular applicability in the context of discussions surrounding legislation like REAL ID, and the concept of unfunded mandates. It is generally in relation to the impact of federal legislative and regulatory requirements that many argue impose unfunded mandates on states. An “unfunded mandate” according to one source is defined as the following.

A requirement set forth by a governing agency that does not provide any type of funding to facilitate the requirement. For example, “In order to comply with the unfunded mandate on security upgrades, the business will have to incur out-of-pocket expenses.”²²⁴

In a sense, an unfunded mandate can be seen by those who see a growth in federal intrusions into state sovereignty as adding insult to injury because it is viewed as imposing significant costs on states in addition to intruding upon the states through requirements that they are powerless to resist. This argument is commonly raised by critics of REAL ID, and has been stressed by one of the more vocal organization critics, EPIC.

EPIC is among the principal opponents of REAL ID, and one that claims that REAL ID is an unfunded mandate on the states. EPIC issued a review of the proposed implementation of the REAL ID Act, in May 2008. In its May 2008 review of REAL ID, EPIC first took issue with the statement from DHS that REAL ID was a voluntary program and not mandatory.

²²³ Garcia, Lee, and Tatelman, *Immigration*, 2.

²²⁴ “What Is Unfunded Mandate? Definition and Meaning,” accessed December 16, 2013, <http://www.businessdictionary.com/definition/unfunded-mandate.html>.

The Department of Homeland Security has repeatedly stated that REAL ID is not mandatory; therefore, it is not an unfunded mandate. However, in EPIC's May 2007 comments on the draft REAL ID regulations, we explained the reasons why REAL ID is not a "voluntary" program.²²⁵

EPIC's argument that REAL ID imposes a mandate and is not voluntary stems not from any statutory or regulatory requirement for the states to comply, but rather from the pressure it claims is being applied to states and individuals. According to EPIC, states feel considerable pressure to implement REAL ID, particularly in the wake of DHS officials remarking that states that do not comply pose a risk to the nation. EPIC also points to the inconvenience faced by citizens in everyday transactions, such as air travel.²²⁶ In addition to the voluntariness aspect, EPIC also takes issue with the inadequacy of financial assistance provided by DHS, noting that DHS allocated \$360 million to the states for implementation effort, an amount that, according to EPIC, pales in comparison to the estimated 9.6 billion estimate for implementation.²²⁷ EPIC is making two separate but related points. One is the voluntariness aspect, and the second criticism that seems applicable relates to the costs imposed on the states, regardless of whether REAL ID is a mandated program. These two points are addressed in turn.

It appears that at most, on the issue of pressure exerted by DHS, the strongest condemnation it can make of DHS efforts to persuade states is DHS' statement that states may find noncompliance "an unattractive option" because of the inconvenience that citizens from noncompliant states would experience.²²⁸ EPIC's assertion that that DHS' expectation of "widespread" acceptance and the continued pressures and penalties on states cause it to remain convinced that the program is not voluntary.²²⁹

²²⁵ EPIC: *Real ID Implementation Review*, 4.

²²⁶ EPIC: *Real ID Implementation Review*.

²²⁷ *Ibid.*, 21.

²²⁸ *Ibid.*, 5.

²²⁹ *Ibid.*

A. THE UNFUNDED MANDATES REFORM ACT

First, it must be understood that federal mandates, or requirements imposed on states or private entities that impose obligations or actions, are not necessarily prohibited, and is embodied in the legislation enacted to offer relief to states, localities, and business entities from unfunded federal mandates. That legislation is known as the Unfunded Mandates Reform Act of 1995 (UMRA).²³⁰

The purpose of UMRA was to establish requirements for legislation and regulations that imposed enforceable duties on state, local, tribal governments or the private sector.²³¹ To understand the issues better, a basic overview and background of the relevant legislation is warranted. Under UMRA, obligations imposed on state, local, or tribal governments, or on the private sector, are referred to as “mandates.”²³² Further, the direct costs to entities required to meet the mandates are referred to as “mandated costs” which become “unfunded mandates” when the federal government does not cover those costs.²³³ The concern with unfunded mandates on the part of state and local entities arose in the 1970s, which was a period of extensive legislative activity on the part of the federal government in furtherance of various federal programs and activities. Many requirements or mandates imposed in furtherance of various government objectives were seen as being in furtherance of the national interest, such as a variety of social welfare programs.²³⁴

The reason that the states and localities became concerned was that during this same period, the federal government shifted from its traditional reliance on “grant-in-aid” programs, which, in effect, subsidized states’ voluntarily efforts in furtherance of those programs, and instead, shifted to a model of imposing requirements under threat of civil fines or criminal penalties.²³⁵ State and local entities, and eventually, business entities as

²³⁰ *Unfunded Mandates Reform Act of 1995*, Public Law 104–4, 109 Stat. 48, 104–4, 1995, 2.

²³¹ Robert Jay Dilger and Richard S. Beth, “Unfunded Mandates Reform Act: History, Impact, and Issues,” 2013, <http://www.fas.org/sgp/crs/misc/R40957.pdf>, 1.

²³² Dilger and Beth, *Unfunded Mandates Reform Act*.

²³³ *Ibid.*, 1.

²³⁴ Dilger and Beth, *Unfunded Mandates Reform Act*.

²³⁵ *Ibid.*, 1–2.

well, mobilized against what they viewed as increasingly compulsory programs, viewing them as contrary to principles of federalism, which was viewed as encompassing cooperation, not compulsion, between the federal government, and state and local entities.²³⁶ This concern, in turn, fueled an effort by the states and localities, as well as business, to seek legislation to control the unfunded mandates. That effort culminated in UMRA, seen by supporters as a restoration of the balance between the federal government, and state and local entities, and a return to traditional principles of federalism.²³⁷ Opponents, however, viewed such mandates as necessary when voluntary actions by local governments or business failed to achieve the desired results.²³⁸

UMRA identified eight statutory purposes to achieve its goal of addressing unfunded mandates. In general, the legislation sought to restore a partnership relationship between the federal government, and state, local, and tribal governments. It further established mechanisms by which greater information was made available regarding the anticipated effects and impact of legislation and regulations on those governmental and non-governmental entities that would be impacted by the complying with or implementing such mandates. It also sought to ensure that informed and deliberate decisions would be made by Congress regarding imposing mandates in any particular instance, and sought to have Congress consider whether it should provide funding. UMRA further required analyses of the impact of federal mandates, and created a procedural mechanism, i.e., a “point-of-order” vote in each chamber of Congress when considering legislation containing significant mandates without providing adequate funding for the entities subject to the legislation to comply.²³⁹

More stringent requirements are placed on the federal government for legislation and regulations that under the law are considered to be “covered mandates,” i.e., those which are *fully* subject to UMRA. Those additional requirements include an assessment from the Congressional Budget Office of the costs imposed on the local entity or

²³⁶ Dilger and Beth, *Unfunded Mandates Reform Act*, 2.

²³⁷ Dilger and Beth, *Unfunded Mandates Reform Act*.

²³⁸ *Ibid.*, 2.

²³⁹ *Ibid.*, 3.

business, which is subject to the covered mandate in proposed legislation, and a similar assessment from the federal agency when regulations are proposed. In addition, for laws considered a “covered mandate” on intergovernmental entities (but not on private entities), UMRA provides for a “point of order”—to each chamber of Congress—which allows each chamber to decline to consider the legislation because of its effect as an unfunded mandate.²⁴⁰

B. APPLICABILITY OF UMRA

UMRA generally applies to “any provision in legislation, statute, or regulation that would impose an enforceable duty upon state and local governments or the private sector.”²⁴¹ However, the law provides for exceptions, and they are broad. It does not apply to “conditions of federal assistance, duties stemming from participation in voluntary federal programs, rules issued by independent regulatory agencies, or legislative provisions that cover individual constitutional rights, discrimination, emergency assistance, grant accounting and auditing procedures, national security, treaty obligations, and certain elements of Social Security legislation.”²⁴² It would seem that REAL ID would arguably be covered under both the voluntary federal programs exception, as well as the national security exception. However, the issue is complex, and clarity on the concept of what constitutes an unfunded mandate has not been achieved given the historically “strong disagreements, among academics, practitioners, and elected officials over how to define it.”²⁴³ Nevertheless, when Congress sought to define “unfunded mandates” under UMRA, it defined it more narrowly than many state and local government officials had hoped.²⁴⁴

While the applicability of UMRA to REAL ID seems doubtful, one benefit of UMRA for REAL ID, and other legislation deemed to be imposing costly and burdensome requirements on states, it does appear that UMRA has had the salutary effect

²⁴⁰ Dilger and Beth, *Unfunded Mandates Reform Act*, 1.

²⁴¹ *Ibid.*, 4.

²⁴² *Ibid.* citing 2 U.S.C. sections 658(5)(A), (7)(A) and ((10), and 2 U.S.C. section 1503.

²⁴³ *Ibid.*, 5.

²⁴⁴ *Ibid.*

of bringing increased attention to the fiscal effects of federal legislation and has fostered greater consultation and collaboration.²⁴⁵ It may also have served as a check on legislation either not proposed, or modified in some way. In support of this point, it is noteworthy that as of August 2013, pursuant to UMRA, the Congressional Budget Office has submitted 9,737 written cost estimates to Congress examining the costs imposed by specific bills, amendments, or conference reports on the private sector or state and local entities. Of those, 1,238 were found to have intergovernmental mandates. Only 13 of those in which the costs exceeded statutory threshold amounts were enacted.²⁴⁶ Among those laws were the predecessor provisions to REAL ID, within the Intelligence Reform and Terrorism Prevention Act of 2004.²⁴⁷ Those provisions, like REAL ID, required that “state and local governments meet certain standards for issuing driver’s licenses, identification cards, and vital statistics documents” and estimated to cost those governments more than \$100 million between 2005 and 2009, with thresholds being exceeded in at least one of the years.²⁴⁸

As for its effect on REAL ID, it is clear that it did not prevent the legislation, and no litigation appears to have ensued that has successfully challenged REAL ID on that basis. It remains possible, of course, that states that have refused to comply might seek to bring such a challenge in the future, particularly when the graduated enforcement measures begin to take effect, and result in the rejection of non-compliant identification documents issued by states. It seems likely, however, that many years after its enactment, and after the expenditure of considerable time, effort, and money at both the federal and local level, that the act would not be struck down, nor would the courts be too likely to interfere in making radical changes to the program or to the federal government’s obligations.

²⁴⁵ Dilger and Beth, *Unfunded Mandates Reform Act*, 19–20 referencing observations by the National Conference of State Legislatures.

²⁴⁶ *Ibid.*, 20.

²⁴⁷ *Ibid.*, 21.

²⁴⁸ *Ibid.*

Nevertheless, the practical issue of concern raised by EPIC is how the states are going to pay for all of the changes to the driver license and identity document issuance systems, which is an issue of practical concern that needs to be addressed. It is obviously in DHS' interests to have states be in a position to make the changes resulting from REAL ID. It should come as no surprise that the states and localities feel burdened by federal mandates and resist the loss of local control. The issue of federal mandates and regulation was discussed at a recent forum undertaken by for the Governance Matters segment of the State and Local Government Review with representatives of state and local government associations (the National Governor's Association, National Association of Counties and National League of Cities).²⁴⁹ That forum, focused on current governance challenges for state and local government entities asked the association representatives to discuss their experience with the federal government on federal mandates. These officials do see a role for the federal government in terms of standard setting, but are of the view that the federal government can best assist those efforts by providing the necessary resources to assist the states and localities in getting the work done. A consensus was reached on this point among the participants, and REAL ID was cited as an example by John Thomasian, Director of the Center for Best Practices of the National Governor's Association, one of the participants in the roundtable discussion:

Most of the fights have been about regulations that have no money behind them. Take the 'Real ID' legislation, for example. This created a massive burden for States that they did not want, with little money to do it.²⁵⁰

The next chapter addresses the funding that has been made available to states for REAL ID implementation.

²⁴⁹ Bruce J. Perlman, "Governance Challenges and Options for State and Local Governments," *State and Local Government Review* 42, no. 3 (December 1, 2010): 246–257, doi:10.1177/0160323X10390050.

²⁵⁰ *Ibid.*, 252.

C. CONCLUSION

Significant opposition to REAL ID comes from states and organizations that see REAL ID as a usurpation of authorities reserved to the states, and as an unfunded mandate. These issues particularly appear to drive the opposition of states that have pursued legislation and other state level actions designed to defy REAL ID openly. While the federal government may ultimately prevail in its efforts to resist challenges based on the Tenth Amendment and unfunded mandates, the resulting battles may come at the expenditure of goodwill and collaboration on an effort that should be seen as mutually beneficial. In addition, failing to respond to, or address this concern could result in states lobbying Congress to loosen REAL ID standards.

How to remedy this situation is unclear, and some states will nonetheless oppose federal efforts in this regard. Another factor in the opinion of those who deal regularly in intergovernmental relations (IGR) appears to be the deteriorating state of dialogue and trust between the different levels of government.

According to our experts, the state of IGR could be better. Unfortunately, they do not believe that it is getting better. Moreover, due to the strains of the recession and reconfigured federal programs, it may be getting worse. All of them see this as an accelerated but not new phenomenon and crucial for State and Local, as well as Federal policies to work. Moreover, the fault is mostly the Federal Government's in their view.²⁵¹

As noted by one participant in the Government Matters forum:

The federal government has spent twenty to thirty years breaking the IGR system. It's now at the point where officials at the different levels of government do not know how to talk to each other anymore.²⁵²

While the federal government may win the battle, it also needs to win the war. Doing so in relation to the struggle between federal and state authority will entail recognizing that the states are largely concerned with resources and some a degree of autonomy in terms of how they address vulnerabilities in state licenses and identity documents. In that regard, DHS and the federal government's efforts should be aimed at

²⁵¹ Perlman, "Governance Challenges and Options for State and Local Governments," 250.

²⁵² Ibid., 250–251.

promoting compliance among the states with a mix of steady pressure to adopt the REAL ID standards coupled with flexibility, such as DHS has demonstrated to date. More importantly, however, DHS should aid the states by improving the tools that states can access to undertake the verification required by REAL ID, but also through direct grants and funding to give states the autonomy to improve their document issuance procedures. The next chapters discuss some of the assistance provided to states to facilitate compliance, the flexibilities afforded them to date, and how DHS seeks to manage enforcement efforts to get the states to the point of full compliance.

VI. TOOLS AVAILABLE TO ASSIST WITH IMPLEMENTATION

A. DHS' SUPPORT FOR VERIFICATION PROGRAMS

In addition to the state specific grants, DHS has provided approximately \$63 million to support verification technology infrastructure solutions including the development of a state-to-state system to address cross-state license fraud.²⁵³ These improvements allow the states to fulfill a key requirement of REAL ID, that a state “shall verify with the issuing agency, the issuance, validity, and completeness of each document required to be submitted by that person.”²⁵⁴ While the local state-grant programs will assist the state in complying, the development and improvement of mechanisms to improve verification require federal oversight and support for common solutions. The need for the verification tools predates REAL ID, and both the states and the federal government have sought to verify the validity of documents for other reasons. For example, the need to verify information presented for individuals to qualify for state and federal benefits, or to demonstrate lawful status in the United States has led to the development of such verification systems.²⁵⁵

The following major systems and/or service providers, which pre-date REAL ID, facilitate key regulatory requirements of REAL ID, with the relevant provision referenced.

- (1) The Systematic Alien Verification for Entitlements (SAVE) system. (States shall verify DHS documents through SAVE 6 CFR 37.13(b)(1))
- (2) The Social Security Online Verification (SSOLV). (States must verify SSNs with the Social Security Administration 6 C.F.R. 37.13(b)(2))
- (3) National Association of Public Health Statistics and Information Systems (NAPHSIS) and the Electronic Verification of Vital

²⁵³ U.S. Government Accountability Office, *Driver's License Security*.

²⁵⁴ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, August 28, 2012, 15 citing *REAL ID Act* Section 202(c)(3)(A).

²⁵⁵ *Ibid.*, 13, 15.

Events (EVVE) application; (States must verify birth certificates presented by applicants 6 C.F.R. 37.13(b)(4))

- (4) American Association of Motor Vehicle Administrators (AAMVA)/AAMVAnet. (States must verify REAL ID driver's licenses and identification cards with the state of issuance 6 C.F.R. 37.13(b)(5)) and (prior to issuing a REAL ID driver's license DL or ID, a state must check with all other states to determine if the applicant holds another driver's license or ID in another state²⁵⁶)

The verification of driver's licenses among states has proven to be a particular challenge for the states, which is necessary to fulfill item 4, above; the REAL ID requirement that states ensure that applicants do not hold licenses in other states. The Government Accountability Office (GAO) touched on this issue in its 2012 report entitled, *Driver License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*. GAO distinguished between two types of license fraud requiring state verification activities. One form is in-state license fraud, which GAO noted was generally addressed by states using facial recognition programs.²⁵⁷ The second type of fraud is cross-state fraud, meaning fraud that occurs across state lines and involves the surrender of licenses from the holder's previous state, which is committed by surrendering fraudulent licenses.²⁵⁸ This type of fraud is beset addressed using a photo-sharing program among the states. Thus, when a license is surrendered in the states in which the applicant seeks a new license, the image is cross-checked against the photo data of the state of original licensure. If no image exists, or if a different image is found that matches the applicant, then fraud is indicated.²⁵⁹ The state-to-state system could also detect the existence of licenses in other jurisdictions that have not been divulged.²⁶⁰ However, limitations to the ability of states to detect this type of fraud exist because a complete state-to-state system is not in existence although progress is being made. As GAO indicated, 23 states and the District of Columbia were participating in a photo-sharing

²⁵⁶ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 15–16.

²⁵⁷ U.S. Government Accountability Office, *Driver's License Security*, 12.

²⁵⁸ Ibid.

²⁵⁹ Ibid.

²⁶⁰ Ibid., 23.

program facilitated by AAMVA.²⁶¹ GAO also noted that state efforts are underway to develop a solution to cross-state licensing fraud using a state-to-state verification system. However, a pilot was not envisioned until 2015, with a fully populated system not anticipated until 2023.²⁶² Until then, the more limited AAMVA program can address some of this fraud, but AAMVA has stated that it lacks the resources to expand the program to other states.²⁶³

B. AN OVERVIEW OF THE VERIFICATION SYSTEMS

Figure 2 shows the various electronic data validation and verification capabilities. Notably, the states proposed the architecture, which was endorsed by DHS and other federal agencies.²⁶⁴ It demonstrates how the various state and federal agencies and public associations and service providers interact and facilitate the verification of information between the service users and data owners. On the left side of the illustration are the state vital records agencies (VRAs), and the state driver license agencies (DLA), which verify the documents they receive through the service providers NAPHSIS and AAMVA, which, in turn, access information maintained by the data owners to provide verification to the VRAs and DLAs.

²⁶¹ U.S. Government Accountability Office, *Driver's License Security*, 12.

²⁶² *Ibid.*, 18–19.

²⁶³ *Ibid.*, 19.

²⁶⁴ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 17.

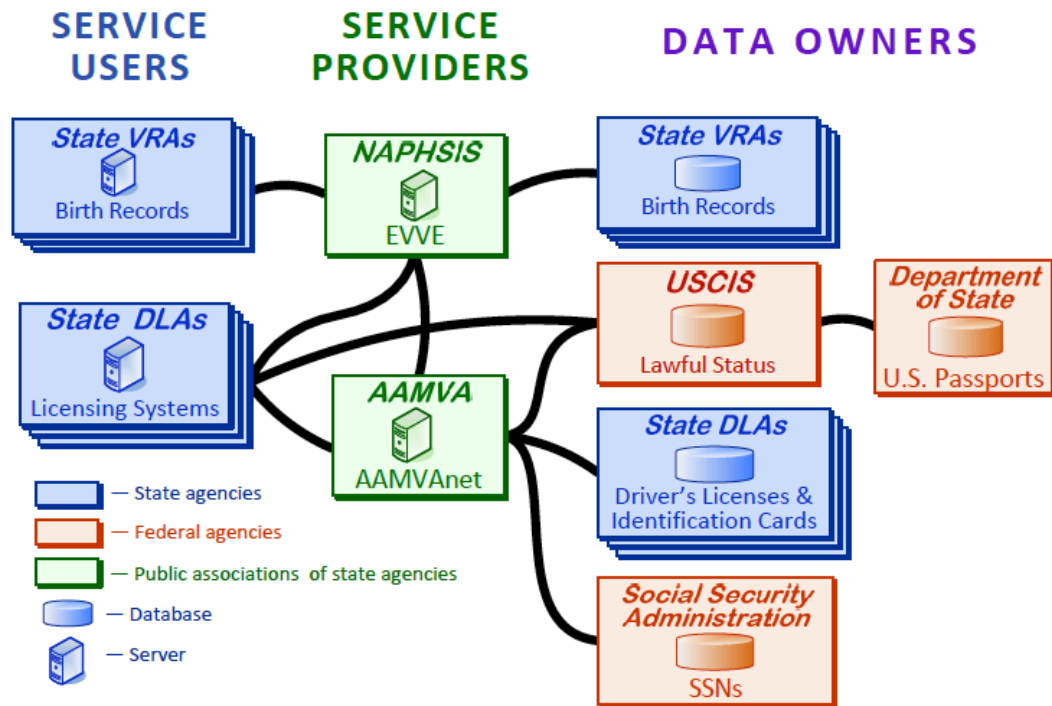


Figure 4. Infrastructure Solution for Electronic Data Validation and Verification

Figure 2. Infrastructure Solution of Electronic Data Validation and Verification²⁶⁵

Through its funding and support of these systems, DHS has improved and strengthened the capability of the service providers to verify the information in an accurate and timely way.

C. INCREASING PROGRESS TOWARD AN EFFECTIVE AND SECURE VERIFICATION SYSTEM

Verifying Immigration Documents/Status

Figure 3 shows that as of February 2012, 47 states have memoranda of agreements (MOAs) in existence with USCIS for access to the SAVE system. SAVE is used to verify immigration status that determines eligibility for state and federal benefits in other contexts, and in the REAL ID context, assists in fulfilling the requirement to

²⁶⁵ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 15.

verify DHS documents, which in turn, demonstrate the immigration status of the individual.²⁶⁶

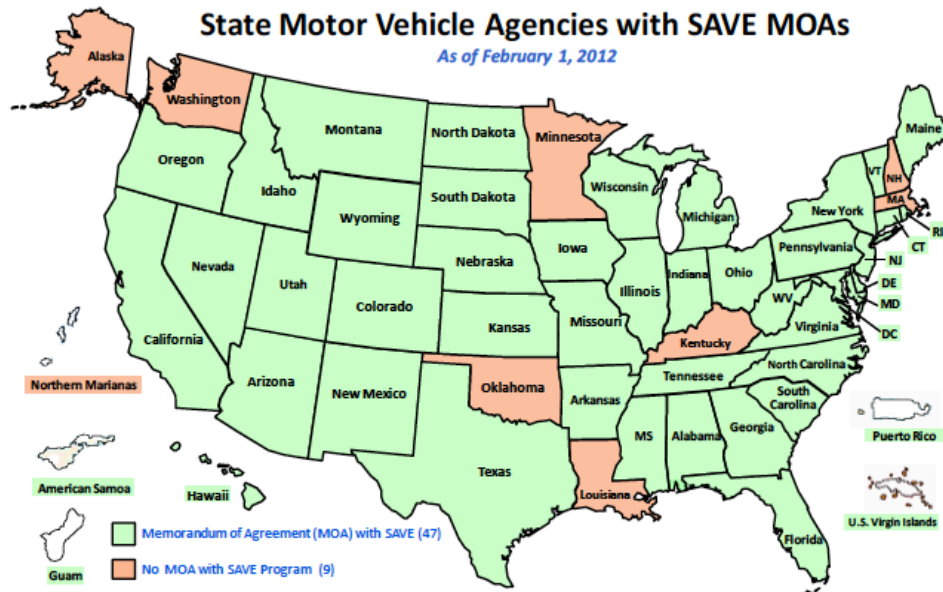


Figure 7. States With SAVE Memoranda of Agreement

Figure 3. States with SAVE Memoranda of Agreement²⁶⁷

States do pay a fee to access SAVE through memoranda of understanding (MOUs) with SAVE (via USCIS), but for a two-year period, a pilot project was being launched to allow states to access SAVE via AAMVAnet for them to integrate SAVE into their frontline operations.²⁶⁸ During that time, funding operations and maintenance of the system would be handled by the State of Mississippi, which is being done to incorporate SAVE into the state operations to make the verification process smoother for

²⁶⁶ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 21. Since SAVE can address and verify only information related to U.S. citizens who possess DHS documents, such as certificates of naturalization, efforts are underway for USCIS to develop and pilot test a service that would verify U.S. passports to provide a conduit through USCIS to information maintained by the Department of State, which is responsible for passport issuance.

²⁶⁷ Ibid.

²⁶⁸ Ibid.

the states. USCIS is assisting in developing a way to allow states to access SAVE through the AAMVAnet communications network.²⁶⁹

Verifying Social Security Numbers

AAMVA developed what is known as the SSOLV system, under the authority of the SSA, to support real-time verification of SSNs.²⁷⁰ As shown in Figure 4, all 50 states and the District of Columbia require that SSNs be verified and use SSOLV. Two states were added since the publication of the REAL ID regulations, and the regulations extended the requirement for verification to the territories. Efforts are underway to extend access to the SSOLV system through AAMVAnet.²⁷¹



Figure 6. Verification of Social Security Numbers

Figure 4. Verification of Social Security Numbers²⁷²

²⁶⁹ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*.

²⁷⁰ *Ibid.*, 19.

²⁷¹ *Ibid.*, 19–20.

²⁷² Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 20.

Verifying State Birth Certificates

The ability to verify state birth certificates is key to the success of REAL ID. It also poses some of the most difficult challenges due to the inability to access electronic copies of records, and the poor quality of such records. For this reason, DHS has paid particular attention to this issue and has funded projects to improve access to such records.²⁷³ It has been recognized that the issuance of driver's licenses has depended on the weak link of "breeder" or "seed" documents. The birth certificate, in particular, is often the least reliable document "because agencies have not kept consistent records and because the documents take so many different forms."²⁷⁴ NAPHSIS supports states in verifying state vital records through a system known as EVVE application, which is most easily accessed by state Department of Motor Vehicles (DMVs) through the AAMVA network. Consequently, DHS is providing funding for projects to improve the accessibility of such records, improve the quality of the records, and correct errors in the data. As shown in Figure 5, the use of EVVE is widespread and growing.²⁷⁵ EVVE allows the states (and other entities, such as the federal government) to connect to EVVE to include digitized vital record checks into their identity verification processes. Technically, the states are not required to conduct such checks, and can claim compliance with the required security benchmarks of REAL ID, without them, but the intent of the federal government is that EVVE be used for that purpose. As a result, it has been funding the installation of EVVE to facilitate access by the states. Under REAL ID, \$3.8 million in funding was provided for this purpose.²⁷⁶ Part of the process for the states involves digitizing older records and cleaning up existing records.²⁷⁷ As a result of REAL ID, digitized identity verification through EVVE, as of December 2013, is used by

²⁷³ Ibid., 22.

²⁷⁴ Kelly Gates, "The United States REAL ID Act and the Securitization of Identity," in *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, ed. Colin J Bennett and David Lyon (London; New York: Routledge, 2008), 227.

²⁷⁵ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 23.

²⁷⁶ Center for Immigration Studies, "Update on Digitization of Vital Records," accessed February 5, 2014, <http://cis.org/kephart/evve-update>.

²⁷⁷ Ibid.

50 states and territories, with two additional jurisdictions in progress (Maine and Puerto Rico).²⁷⁸

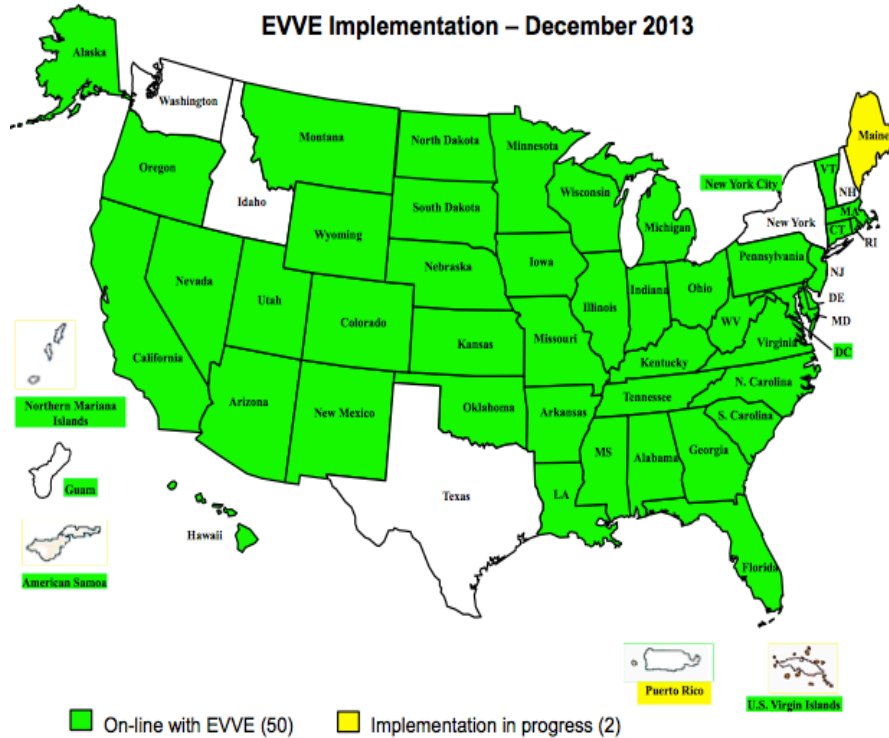


Figure 5. EVVE Implementation—December 2013²⁷⁹

A significant increase occurred from the implementation status as of June 2012, contained in the DHS state progress update, which showed that 43 states and territories were online, six were in progress, and eight had yet to begin any implementation.²⁸⁰ (See Appendix B.)

However, five states (New York, Texas, Washington, Idaho, and New Hampshire) have not yet accessed vital records through EVVE, which represents a

²⁷⁸ NAPHISIS, “EVVE,” accessed February 5, 2014, <http://www.naphsis.org/Pages/EVVE.aspx>.

²⁷⁹ NAPHISIS, “EVVE.”

²⁸⁰ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 23.

substantial number of driver's licenses and state identification documents.²⁸¹ This tool has seen a substantial increase in use among states and territories since the creation of the EVVE office 2005. As recently as February 2011, only 28 states were online with the EVVE system.²⁸²

An additional digitization effort that would identify additional fraud involves linking digitized birth and death records in the system. It has been estimated that the cost to do so would be approximately \$102 million.²⁸³ One area of opportunity for the federal government to assist states would be to pursue funding for such efforts. The IRTPA's Section 7211 authorized federal grant programs that would help states to "meet federal standards." Although the authorization to appropriate funds ran out in 2009, it would be worthwhile to pursue the reauthorization of such grants, and seek appropriations to fund the grants.²⁸⁴

D. CHAPTER CONCLUSION

Many critics of REAL ID indicate that states are incapable of verifying the documents presented to them, but as discussed above, cooperation between states and the federal government has significantly strengthened such capabilities. Due to the need for states to verify eligibility for state or federal benefits, systems had already been developed to facilitate verification. Since REAL ID was enacted, steady and ongoing progress continues, and additional efforts are being made to improve state access to the systems.

The tools to assist states with complying with REAL ID exist, and are widely available, although improvements are necessary and continue to be made. Aside from increasing the ability of states to verify documents for purposes of the REAL ID

²⁸¹ It is not apparent from the information reviewed to date, why New York and Texas are not yet tied into the EVVE system, given the volume of transactions and their vulnerability to fraudulent documents. It would not seem to be attributable solely to size, since California *is* tied into the system. Given the risks posed by fraudulent documents, and the risks to New York, in particular, this anomaly merits additional research.

²⁸² Center for Immigration Studies, "Update on Digitization of Vital Records."

²⁸³ Ibid.

²⁸⁴ Ibid.

requirements, these tools serve another valuable purpose, which is also key to the utility of REAL ID. They assist the states in addressing fraud committed using fraudulent state, and immigration documents, passports, and Social Security cards.

VII. FUNDING ASSISTANCE AND FLEXIBILITY ON DEADLINES FOR THE STATES

The final rule sets out the law's requirements, It also addressed the more than 21,000 public comments received, many of which focused on the costs to the states. The final rule indicated that DHS had made changes from the proposed rules to assist the states in addressing costs. First, DHS indicated it was making approximately \$360 million available to assist states with \$80 coming from direct REAL ID grants, and an additional \$280 million in general funding as part of the Homeland Security Grant Program. It also announced that costs were reduced by 73 million due to measures that were taken in the final rule to address costs, i.e., giving the states additional flexibility in issuing licenses to older Americans. This flexibility would allow states to enroll individuals younger than 50 until December 1, 2014, while enrollment of other individuals would be required by December 1, 2017, at which time, state-issued licenses and ID cards that were non-compliant with REAL ID, would be rejected for any official federal purpose.²⁸⁵

A. EXTENSIONS OF COMPLIANCE DATES AND A MOVE TOWARD ENFORCEMENT

1. A Series of Extensions

The law, as originally designed, required states to comply with REAL ID by May 11, 2008. Through a series of at times confusing regulatory waivers and extensions, the full compliance deadline was ultimately moved to January 15, 2013, with an announcement being made in December 2013 that DHS would begin enforcing REAL ID in 2014. The complex, but interesting series of communications by DHS, steadily nudged states toward compliance while providing incentives and threatened penalties for non-compliance, merits brief discussion.

The final regulations gave DHS the authority to consider requests for waivers filed by the states and provided that such waivers would be granted, if the state seeking

²⁸⁵ *Department of Homeland Security, Final Rule.*

the extension offered “adequate justification for noncompliance.”²⁸⁶ The final regulations further elaborated upon the extension process that would extend the date by which full compliance was expected, to May 11, 2011, if states seeking extensions were able to meet an interim, material compliance deadline of January 1, 2010.²⁸⁷ (See Appendix C for a Chart on State Compliance Milestones.)

Following the publication of the final regulations, Secretary of DHS Michael Chertoff was very visible in public defending and advocating on behalf of REAL ID. Secretary Chertoff initially took a hard line on compliance and the states’ need to adhere to the deadlines. At one such event, dubbed a “Pen-and Pad Briefing,” Secretary Chertoff responded to a question about what would happen to states that did not meet the deadline. He stated:

What’s going to happen is this. Now, first, let me make it clear. I’m not bluffing about May 11, [the compliance date] and even if I were inclined to be a bluffer, which I’m not, the law makes it clear. The law passed by the Congress is: On May 11th, if you don’t get a waiver, then you’re going to have—a driver’s license will not be acceptable for federal purposes as an ID.²⁸⁸

Thus, DHS allowed states to submit, no later than March 31, 2008, requests for extension that would last until, but no later than December 31, 2009. It seems likely that Secretary Chertoff knew that the states would seek the waivers from compliance and that his main objective may have been to ensure that the states did not simply just ignore the deadline but sought waivers. This objective was achieved, as seen in Figure 6, which shows the jurisdictions that had sought, and were granted, the initial waiver and extension for compliance to December 31, 2009.

²⁸⁶ *The REAL ID Act of 2005*, Section 205(b).

²⁸⁷ Department of Homeland Security, “Final Rule.” (The particular provision regarding extensions was codified at 6 C.F.R. 37.63).

²⁸⁸ Department of Homeland Security, *DHS Press Release: Remarks by Homeland Security Secretary Michael Chertoff at Pen and Pad Briefing on the Department’s Fifth Anniversary*, March 6, 2008.

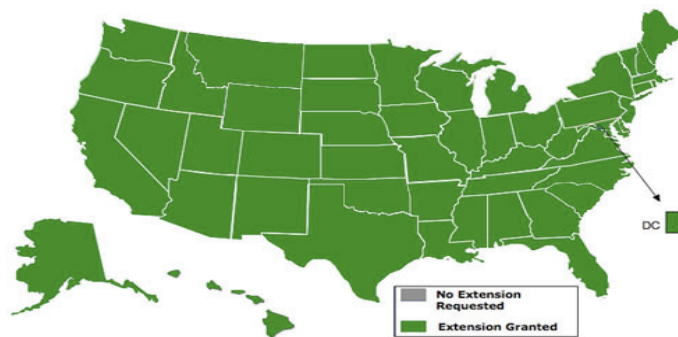


Figure 6. Initial Waiver and Extension for Compliance to December 31, 2009²⁸⁹

As can be seen, all jurisdictions sought, and were granted, extensions by the Bush administration, to December 31, 2009.

Subsequently, DHS, seeing that states would have difficulty achieving full compliance, and in an attempt to give effect to the waiver provision, bifurcated the requirements for states. It kept the full compliance date at May 11, 2011, but allowed states to demonstrate that they were materially compliant by January 1, 2010, based on meeting certain benchmarks. Furthermore, states could seek an extension beyond that date if they submitted, by December 1, 2009, a “Material Compliance Checklist” demonstrating their commitment to complying with the regulations. This was intended to reward states making progress toward compliance.²⁹⁰ (See Appendix D for synopsis of material compliance benchmarks.) If material compliance were demonstrated, the state’s extension would then last until no later than May 10, 2011 for full implementation. DHS, however, learned that 46 of 56 jurisdictions were unable to establish material compliance, and thus, stayed the material compliance deadline through the publication of a final rule in the Federal Register on December 29, 2009, staying the January 1, 2010 material compliance deadline.²⁹¹ DHS’ change to the compliance deadlines had the effect of bifurcating the requirements. First, DHS required states to demonstrate that they were in

²⁸⁹ Stewart Baker, Assistant Secretary for Policy, “Real ID,” March 20, 2008, *DHS Leadership Journal Archive* <http://ipv6.dhs.gov/journal/leadership/labels/Real%20ID.html>.

²⁹⁰ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 4.

²⁹¹ *Ibid.*

material compliance by January 10, 2010, and they would then need to achieve full compliance by May 11, 2011., which was further amended in December 2009, by indefinitely suspending the date by which states had to demonstrate material compliance.

Finally, DHS promulgated a final rule on March 7, 2011 that extended the date for full compliance and change it to January 15, 1013.²⁹² This deadline was not further extended, but DHS then announced its intention to begin a gradual enforcement of the provisions of REAL ID, which it announced in December 2013, and which is discussed next.

2. Enforcement Comes at Last?

Most recently, DHS, on December 20, 2012, announced that it would begin to phase in the enforcement of REAL ID. The announcement indicated it would do so in a phased manner, with four distinct phases of enforcement, the first being restrictions on the use of non-compliant IDs for access to the DHS Headquarters facility, known as the Nebraska Avenue Complex (NAC). The enforcement schedule, set forth below, calls for a graduated enforcement, with each phase beginning with a period of public notice followed by a specified date when full enforcement begins. Each successive enforcement phase carries with it higher level consequence and impact upon the public, and culminates—no sooner than 2016—with full enforcement of the requirement to present REAL ID compliant driver’s licenses for the purpose of boarding federally regulated aircraft.²⁹³ This graduated enforcement, while perhaps excessive in its length, given DHS statements about how close most states are to full implementation, may prove to be a wise approach.

In support of its announcement regarding the phased enforcement, DHS published a brief and helpful overview of the planned enforcement that contained two useful visuals to inform the public and the states regarding 1) its enforcement timetable, and 2) the

²⁹² Government Printing Office, “Federal Register, Volume 76 Issue 44 Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes,” March 7, 2011, <http://www.gpo.gov/fdsys/pkg/FR-2011-03-07/html/2011-5002.htm>.

²⁹³ “DHS Releases Phased Enforcement Schedule for REAL ID.”

current status of state compliance with REAL ID requirements.²⁹⁴ Those visuals are reproduced in Figure 7. The first image is DHS’ chart showing the four phases of implementation, to include the following.

- The four phases of enforcement
- The enforcement action being taken
- The commencement date of public notice
- The commencement date of full enforcement

Phase	Enforcement	Notification Period	Full Enforcement
1	Restricted areas for DHS/NAC	1/20/14	04/21/14
2	Restricted areas for all Federal facilities & for nuclear power plants	04/21/14	07/21/14
3	Semi-restricted for all Federal facilities	10/20/14	01/19/15
<i>Review and Evaluation</i>			
4	Aircraft (Acceptable with 2nd form of ID)	No sooner than 2016	

Figure 7. Enforcement Phases and Dates²⁹⁵

As can be seen, DHS’ plan is to do graduated and cumulative levels of enforcement, beginning with relatively low impact consequences affecting a limited population, and eventually culminating in the restriction of the ability of residents of non-compliant states to use their state issued identification documents for the purpose of boarding federal aircraft. This latter enforcement measure is the most well-known and anticipated consequence with a high impact on the general public. Notably, DHS does not commit to a date certain for that consequence, noting that it would occur “no sooner than 2016.” DHS plans to undertake an evaluation following the implementation of the first three enforcement phases, to “assess the effects of enforcement and the progress of states in meeting the standards of the act.”²⁹⁶ That assessment will inform its decision prior to setting the date for full compliance with phase 4, and will “inform a fair and achievable

²⁹⁴ Department of Homeland Security, “REAL ID Enforcement in Brief,” December 20, 2013, <http://www.dhs.gov/sites/default/files/publications/REAL-ID-IN-Brief-20131220.pdf>.

²⁹⁵ Ibid.

²⁹⁶ Ibid.

timeline.”²⁹⁷ In each phase, DHS plans to precede the particular enforcement mechanism with a three-month advance notification period. How much public education and outreach DHS will undertake during that time remains to be seen. It is anticipated, however, that for a smooth implementation to occur, and to minimize the effects of the enforcement mechanisms, a fair degree of coordination with the states would occur, particularly those not yet compliant with REAL ID.

DHS’ release of its phased enforcement plan was also accompanied by an updated listing of the status of the states and territories showing their status as being either non-compliant or a compliant/extension state. Compliant states are those that have met all of the REAL ID requirements, and extension states are those that have sought extensions, which are currently valid through October 10, 2014.²⁹⁸ As full enforcement begins, residents of compliant/extension states can continue to use their state documents as before, but residents of non-compliant states “will need to follow alternative access control procedures for purposes covered by the Act.”²⁹⁹ Figure 8, supplied by DHS in connection with its announcement of the beginning of phased enforcement sets forth, in an easy to distinguish manner, the non-compliant states from the compliant/extension states.

²⁹⁷ Department of Homeland Security, “REAL ID Enforcement in Brief.”

²⁹⁸ Ibid.

²⁹⁹ Ibid.

A) Noncompliant States/Territories	
Alaska	Montana
Am.Samoa	New Jersey
Arizona	New Mexico
Kentucky	New York+
Louisiana	N. Marianas
Maine	Oklahoma
Mass.	Washington+
Minnesota	
+ Federal officials may continue to accept Enhanced Driver's Licenses from these states.	
B) Compliant/Extension States/Territories	
Alabama	Nebraska
Arkansas*	New Hampshire*
California*	Nevada*
Colorado	N.Carolina*
Connecticut	N.Dakota*
Delaware	Ohio
DC*	Oregon*
Florida	Pennsylvania *
Georgia	Puerto Rico *
Guam*	Rhode Island *
Hawaii	S.Carolina*
Idaho*	S.Dakota
Illinois*	Tennessee
Indiana	Texas*
Iowa	Utah
Kansas	Vermont
Maryland	Virginia*
Michigan *	Virgin Islands*
Mississippi	West Virginia
Missouri *	Wisconsin
	Wyoming
* Has an extension through October 10, 2014(renewable)	

Figure 8. Non-compliant and Compliant/Extension States³⁰⁰

DHS puts a positive spin on the status of the states, noting that as of December 20, 2013, “approximately 75% of all U.S. drivers hold licenses from jurisdictions that have met REAL ID standards, or have received extensions.”³⁰¹ While it is true that those drivers can be assured of no adverse consequences as a result, the reality is that the 75%

³⁰⁰ Department of Homeland Security, “REAL ID Enforcement in Brief.”

³⁰¹ Ibid.

figure comes from 41 states, and of those, 21 have been deemed fully compliant. Adding the number of non-compliant states to the number that are the beneficiaries of extensions, yields a total of 35 states and territories still not in compliance. It is, undoubtedly, DHS' expectation that the extension states will be encouraged to pursue more active measures to bring themselves into compliance during the course of the phased enforcement. The greater challenge, of course, is to persuade those non-compliant states, particularly those that are defiantly so, to pursue the necessary steps to come into compliance. The possibility—or even the likelihood—also remains of a confrontation, likely in the form of a legal challenge sometime down the line on the part of some or all the states that continue to oppose the REAL ID requirements. While this author believes that the likelihood of success of such a challenge is low, the fact remains that a victory for DHS many years down the line will simply result in significant delays in shoring up weaknesses in the nation's license and non-driver license identification system. Those weak links have been, and will continue to be exploited by those who mean harm to individuals, institutions, and possibly, to the nation's security.

B. CHAPTER CONCLUSION

Given the enormous scope and the complexity of the task for the states to come into full compliance, and the internal dynamics within states in addressing REAL ID, it is not surprising that the regular extension requests were made, and subsequently, granted.

Although it is not clear that these requests were done for this reason, granting the extension requests it also appears, in retrospect, to have been a move that may ultimately help to achieve full compliance. Moreover, it has been the back and forth between the states and the federal government, and the measures taken by both in fashioning responses to the legislation that reflects the truly interesting evolution regarding driver's license and identification card security. Compliance could not be achieved without substantial effort on the part of both the states and the federal government.

VIII. FINANCIAL SUPPORT PROVIDED BY DHS TO THE STATES

A. DHS HAS PROVIDED SUBSTANTIAL SUPPORT TO ENCOURAGE COMPLIANCE BUT THE TRUE COSTS OF REAL ID IMPLEMENTATION ARE UNKNOWN

Under the REAL ID Act, the Secretary of Homeland Security is authorized to make grants to states to assist them in conforming to the law's minimum standards.³⁰² In addition, Congress authorized to be appropriated for each fiscal year (FY) from 2005 through 2009, "such sums as may be necessary to carry out this title."³⁰³ DHS addressed the cost issue in a press release dated January 11, 2008, accompanying the announcement of the impending publication of the final rule, noting that DHS was making \$360 million available to assist states with REAL ID implementation. Of that total, \$80 million would be in the form of dedicated REAL ID grants and another \$280 million would be in the form of general funding under the Homeland Security Grant Program.³⁰⁴

Congress and the Executive Branch both recognized that compliance with REAL ID was going to require considerable funding at both the federal and local level. Substantial changes were being required of the state DMV system regarding their issuance of driver's licenses and identity documents. Those changes included modifying procedures and making the necessary technical modifications to facilitate identity and document verification requirements. During the rulemaking process, DHS published a substantial treatment of the costs associated with REAL ID in its regulatory evaluation accompanying the final rule. DHS indicated that the evaluation provided a "comprehensive, rigorous, and exhaustive" evaluation of the benefits and costs of the final minimum standards for state-issued driver's licenses and non-driver identification cards under REAL ID.³⁰⁵

³⁰² *The REAL ID Act of 2005*, 302.

³⁰³ *Ibid.*

³⁰⁴ Department of Homeland Security, *DHS Releases REAL ID Regulation*, January 11, 2008.

³⁰⁵ Department of Homeland Security, *Regulatory Evaluation Final Rulemaking 6 CFR Part 37*, January 17, 2008, 1.

In estimating the costs, DHS noted that REAL ID implementation reflected a joint state, federal, and public effort that would be executed over an 11-year period of time. Overall, DHS estimated the 11-year cost of the final rule at “less than \$10 billion, of which less than \$4 billion are States costs” and determined that it would result “in an average marginal cost of \$8.31 per card issuance to the States.”³⁰⁶ The DHS assessment anticipated that two phases of expenses would be necessary. The first phase would encompass years one through four during which time states would be making changes to their business process and making investments to meet the standards of REAL ID, with states working to meet standards of material compliance and beginning to enroll applicants by January 1, 2010.³⁰⁷ The second phase would encompass years four through eleven, during which time states would continue to enroll applicants and would begin issuing fully compliant licenses no later than May 11, 2011.³⁰⁸ DHS noted between the time of the notice of proposed rulemaking and the final rule, that it had adjusted some of its assumptions, which resulted in reallocating certain costs or reducing it in others. For example, DHS recognized that “most if not all” states would be unable to meet the May 2008 deadline, and would seek extensions, which would necessarily redistribute costs to subsequent years.³⁰⁹ DHS also adjusted its assumption that 100% of the candidate population would seek REAL ID compliant documents, instead determining that 75% would do so.³¹⁰ The brief treatment in this paper of the regulatory assessment and the combined organization estimates of the costs does not begin to explain the complexity and detailed treatment of the costs, and the assumptions made and findings adopted by DHS. Those interested in having a better understanding of the complexity and detailed work that went into that assessment should consider reading the entire regulatory assessment document. (See Appendix E for the extended Table of Contents of the Regulatory Evaluation)

³⁰⁶ Department of Homeland Security, *Regulatory Evaluation Final Rulemaking 6 CFR Part 37*.

³⁰⁷ *Ibid.*, 1.

³⁰⁸ *Ibid.*

³⁰⁹ *Ibid.*, 2.

³¹⁰ *Ibid.*

Aside from the federal government, the states have also provided an assessment of costs. Anticipating the costs that would have to be borne by states, three influential groups with strong interests in REAL ID, had set forth their own estimate of the costs two years earlier. The National Governor's Association, AAMVA, and the National Council of State Legislatures issued a joint report in September of 2006 based on a survey of DMV officials using a 114 multi-part questions survey answered by 47 of 51 DMV officials surveyed. The organization's report found as follows.

Based on the results of that survey, NGA, NCSL and AAMVA conclude that Real ID will cost more than \$11 billion over five years, have a major impact on services to the public and impose unrealistic burdens on states to comply with the act by the May 2008 deadline. The organizations also provide practical and cost effective solutions for Congress and the Department of Homeland Security (DHS) to address these shortcomings and meet the objectives of the act.³¹¹

As can be seen, the report estimated costs of approximately 11 billion for successful implementation, yet it does not break this figure out between costs to the federal government versus costs to the states, which leaves the impression that the organizations considers these to be costs to the states. If so, the estimates are much higher than those estimated by DHS to be costs incurred by states. The report appears to be less detailed and precise and more based upon self-reported estimates by states, which may or may not precisely done, or be estimated on the high side. As will be seen, some believe that the estimated costs were exaggerated. Yet, these early estimates by DMV officials still reflect the considerable costs associated with REAL ID.

It is likely that both the DHS and the state entities missed the true cost, and it is perhaps likely that the federal government's estimates were low, and those of the states and their affiliated organizations were high. While the final costs may never be known, it is useful to examine how much federal aid has been provided to states compared to what the federal government estimated it would cost, and what forms that aid has taken.

³¹¹ National Governors Association, National Conference of State Legislatures, and American Association of Motor Vehicle Administrators, "The REAL ID Act: National Impact Analysis."

B. GRANTS AND OTHER FORMS OF STATE ASSISTANCE

Federal assistance has been provided to the states through three distinct, but integrated assistance programs: 1) FEMA grants totaling approximately \$200 million for individual state projects to improve the security of their documents, facilities, systems and business processes, in a manner consistent with REAL ID, 2) FEMA targeted grants to five states in a demonstration project designed to upgrade the network of state-owned and operated systems that states already use to verify and exchange information with federal and state agencies,³¹² and 3) USCIS support of almost \$10 million in projects to develop and deploy cost-effective methods to verify lawful presence electronically, U.S. passports, and SSNs, pursuant to the requirements of REAL ID.³¹³

DHS, reported in its 2012 progress report that in June 2008, FEMA announced the initial REAL ID grant awards.³¹⁴ (Appendix F is FEMA's notice regarding the availability of the 2008 grant funding that totaled over \$79 million)³¹⁵

Figure 9 shows the number and allocation of grants by DHS to the states. Two states, Montana, and Oklahoma, did not receive grants, as they sought no grants. They took a principled position perhaps, given their declared intention not to adhere to the REAL ID requirements.

³¹² States participating in the demonstration project included Mississippi, Kentucky, Indiana, Florida, and Nevada.

³¹³ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, iii.

³¹⁴ *Ibid.*, 2.

³¹⁵ Federal Emergency Management Administration, *Grant Programs Directorate Information Bulletin No. 277 January 28, 2008: Consolidation of Fiscal Year (FY) 2008 REAL ID Funding Availability*, January 28, 2008.

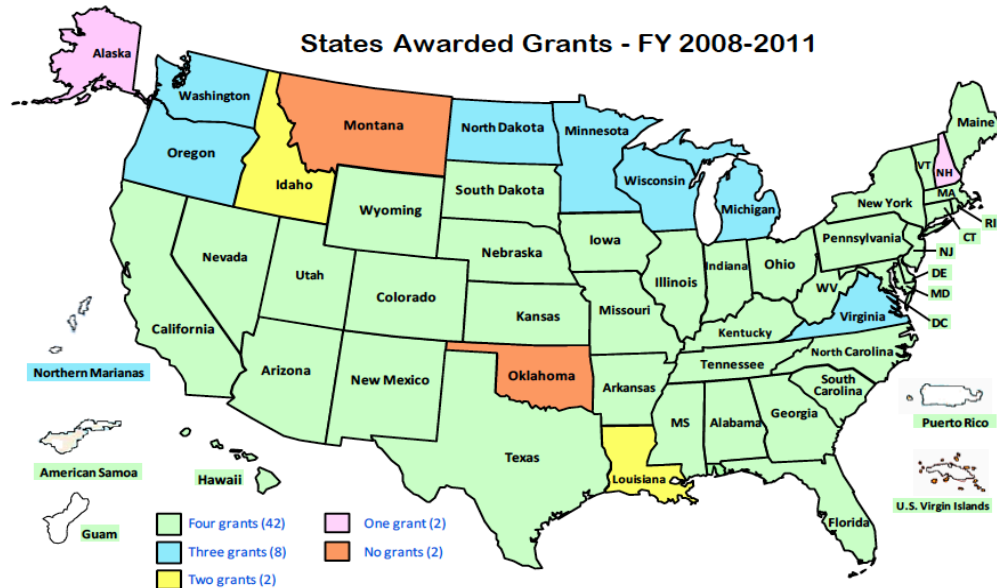


Figure 2. Number of Grants Awarded, FY 2008–FY 2011

Figure 9. Number of Grants Awarded, FY2008–FY2011³¹⁶

The financial support offered to the states by DHS has been substantial although not at the level to cover the full cost originally estimated in the DHS rulemaking, as endorsed by the Congressional Budget Office of the 3 billion estimate associated with state costs. Since 2008, FEMA had awarded the states more than \$263 million in REAL ID and Driver's License Security Grant Program funding. As reported by DHS, the support given to states falls within two types, 1) individual projects, whereby DHS funds projects consistent with REAL ID, and 2) projects identified by the states through grant applications and that encompass a range of improvements at the state level.³¹⁷ The projects supported have encompassed areas such as the following:

- Card security upgrades
- Equipment upgrades
- Facility upgrades
- System and IT infrastructures upgrades

³¹⁶ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 15–16.

³¹⁷ *Ibid.*, 13–15.

- Licenses issuance and business process security upgrades
- Employee programs
 - Training on fraudulent documents
 - Background checks on employees
- Electronic verification and document applicant source documentation
 - Verification of social security numbers
 - Verification of lawful status through use of SAVE program
 - Verification of U.S. passports
- Public service campaigns to educate the public³¹⁸

C. SOME BELIEVE IMPLEMENTATION COSTS MAY HAVE BEEN LOWER THAN ESTIMATED

Nine years after the passage of REAL ID, with the experience of implementation efforts and expenditures to date, it would be prudent to assess the current status of states' costs to implement REAL ID, relative to federal funding needed in the form of grants, and specific appropriations for state and federal implementation efforts. At least one commenter believes that the costs of implementing REAL ID have proven to be much lower than original estimates, and that in fact, in some situations states have returned unspent grant money to the federal government, or have successfully implemented REAL ID at much lower costs than projected. Janice Kephart, a frequent commenter on issues related to REAL ID, who, at the time was the Director of Security Policy at the Center for Immigration Studies, wrote a *Backgrounder* document on REAL ID implementation in January 2011, addressing, among other things, implementation costs as they had developed, relative to the projected costs. She wrote the following regarding the REAL ID implementation costs.

Perhaps most remarkable about REAL ID implementation to date, from the states where REAL ID expenditures have been made public, is that the costs for compliance are coming in nowhere near the \$11 billion price tag that the NGA, NCSL, and AAMVA presented in the 2006 National Impact

³¹⁸ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 14–15.

Statement....This number now appears to have been grossly exaggerated.³¹⁹

She noted that in three states (Delaware, Maryland, and Iowa) the implementation costs were roughly double what the federal government had allocated through federal grants; in other words, in those states, local resources comprised half the implementation cost.³²⁰ Kephart notes that two states, Florida and Alabama, were outliers with Florida apparently being over-funded with REAL ID grants, and Alabama spending over \$15 million, with only approximately \$2 million coming from REAL ID grants.³²¹ If Alabama's costs, which were considerably more, were extrapolated to all states, then, according to Kephart, the cost would, in fact, approach the amount estimated by the National Governors Association (NGA), National Conference of State Legislatures (NCSL) and AAMVA.³²² However, Alabama's situation was not typical, and in her view, it appeared that in most states, the situation would be more like that in Delaware and Maryland, where the states had to contribute about one-half of the implementation costs. For the most part, according to Kephart, state costs have been lower than expected. For those wishing to see a more detailed treatment of this issue, Kephart's article includes a very useful chart that displays, by state, where the state finds itself relative to its connectivity to verification systems, and how much each state has expended to implement REAL ID or achieve its benchmarks. (That chart is reproduced in Appendix G.)

Kephart's principal point is that while outlier states in terms of REAL ID implementation costs do exist, most states will find themselves in situations closer to that of Delaware and Maryland in which the implementation costs were about double the amount given to the states in grants, and in some situations, state implementation costs have roughly matched the grant allocation. She makes the following cogent points relative to Congress' funding of implementation costs going forward.

³¹⁹ Kephart, "REAL ID Implementation: Less Expensive, Doable, and Helpful in Reducing Fraud."

³²⁰ Ibid., 7.

³²¹ Ibid.

³²² Ibid., 7–8.

If Congress feels that splitting the costs with the states is sufficient, then the federal government has fully funded REAL ID at this point. . . If states successfully seek full funding, Congress is halfway there, and full REAL ID implementation is—at least from a financial and technical point of view—doable and in sight. Congress should be careful to look at real cost figures from state Departments of Motor Vehicles before making a decision.³²³

Consequently, it seems that the claim that federal funding of REAL ID implementation costs incurred by states has been grossly inadequate requires a closer examination, and should not be taken at face value as DHS assesses state needs for additional funding.

D. CHAPTER CONCLUSION

A major argument in opposition to REAL ID has been that it was extremely expensive to implement, with the costs falling disproportionately to the states. To add to the difficulty for the states, and the general perception surrounding the issue, the federal regulations became effective in 2008, at the beginning of the economic downturn from which the country has yet to fully recover. Logically, implementation would have placed an additional burden on already stressed state budgets. It is no wonder then, that the challenges between the states and the federal government, fiscally, politically, and in terms of legitimate debates based on federalism principles, set up a perfect storm of sorts for federal state relations related to REAL ID. It seems, however, that an assessment of the true costs of REAL ID implementation, and the proper allocation of those costs between the federal and state governments is in need of a fresh look to determine the proper level of continued aid to the states going forward.

The perceptions about federal efforts to assist the states with funding REAL ID's implementation has been one of the important factors that have affected state views regarding REAL ID and how the states have reacted to the law. To that end, since the law's passage, DHS has provided states with a variety of grants and other means of support to facilitate their compliance. How the states reacted to REAL ID is reflected in the next chapter, which examines state reaction on a macro level, and the subsequent

³²³ Kephart, "REAL ID Implementation: Less Expensive, Doable, and Helpful in Reducing Fraud, 8.

chapter, which examines more closely how three particular states addressed the implementation challenges.

THIS PAGE INTENTIONALLY LEFT BLANK

IX. THE REACTION OF THE STATES TO REAL ID

A. SOME STATES REBELLED

As the previous chapter demonstrated, significant grant money has been awarded to the states, and many states have been working to come into compliance, despite protesting against unfunded mandates and asserting that compliance would be too costly to implement. Nevertheless, many states are still significantly opposed to REAL ID. In fact, it is probably fair to say that several states rebelled against the law and did so not just through the public statements of their elected leaders, such as former Governor Mark Sanford (R-SC) and Senator John Tester (D-MT).³²⁴ They have done so through more substantial measures including legislative enactments and non-binding resolutions. Major concerns of the states have related to the costs of upgrading their license issuance systems and the previously discussed concerns about REAL ID being an unfunded mandate.

In terms of state reaction to REAL ID, some states are more aggressive in demonstrating their opposition to the requirements of REAL ID. The opposition from governors and state officials has spanned across political parties. Two state officials, in particular, Senator John Tester (D-MT), and Mark Sanford (R-SC), were particularly vocal opponents of REAL ID and spoke of their states' opposition to REAL ID at a Cato Institute forum on REAL ID.³²⁵ During the forum, held on May 7, 2008, Senator Tester stated:

Montana's politics features a mix of prairie populism, tax-hating conservatism, and leave-me-alone libertarianism. Some folks even manage to be all of those things at one time. So getting a unanimous vote in the state legislature is a pretty rare thing. But, that is what happened last year when 150 members—100 in the House and 50 in the Senate—joined the governor in opposing REAL ID. There were no votes in favor of REAL ID.³²⁶

³²⁴ Cato Institute, "The Real ID Rebellion" August 2008, <http://www.cato.org/policy-report/july-august-2008/real-id-rebellion>.

³²⁵ Ibid.

³²⁶ Ibid.

Fourteen states have passed legislation prohibiting their states from complying with the provisions of REAL ID. Figure 10, from AAMVA, reflects, in blue, the states that had adopted anti-REAL ID legislation as of August 2012.³²⁷

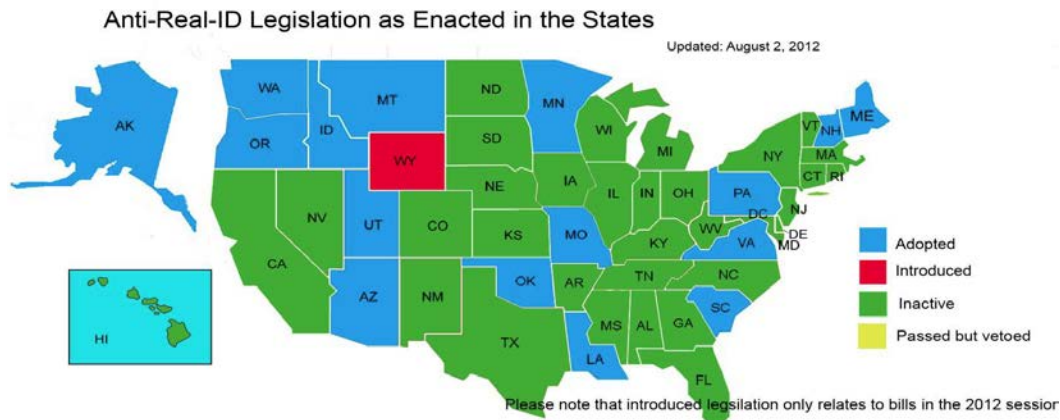


Figure 10. Anti-REAL ID Legislation As Enacted in States

Similarly, the NGA has also been vocal in expressing its views on REAL ID and advocating for additional funding, as well as state involvement in implementing the law. When REAL ID passed in 2005, the NGA issued a statement expressing its opposition to the legislation noting that:

It would repeal the framework that Congress established under the Intelligence Reform Act to involve states in developing workable and effective national standards for state driver's licenses and identification cards;

Several of the requirements, particularly those having to do with verification of documents used to acquire an ID, are either technologically or fiscally prohibitive;

As governors evaluate and review the implications of the unfunded federal mandates imposed by REAL ID, they encourage the U.S. Department of

³²⁷ The American Association of Motor Vehicle Administrators, "2012 State Status of Real ID," August 2, 2012, <http://www.aamva.org/>. This map includes two additional states—Utah and Virginia—as having enacted state laws prohibiting compliance. The discrepancy is not explained in the documents, and further research is necessary to reconcile the difference between the two sources.

Homeland Security to draw upon the expertise and perspective of governors to develop mutually agreed-upon regulations.³²⁸

(See Appendix H for a detailed chart dated from the National Conference of State Legislatures identifying the different types of legislative actions taken by the states as of June 2012).³²⁹ Those actions include legislation enacted; approved concurrent/joint resolutions; and approved House or Senate resolutions. It should be noted that the landscape is constantly changing with states shifting between the different categories depending on the activities of its elected officials. It will also be interesting to observe how it may change as the federal government begins to enforce the REAL ID provisions by rejecting state identification documents for federal official purposes.

When the history of the REAL ID Act and its origins is examined, the partial irony of the states that have defied the REAL ID provisions cannot be escaped when considering the states themselves, through their motor vehicle administrators, were leading the push for enhanced standards for driver's licenses. In response to the 9/11 attacks, AAMVA, which is the umbrella organization for the nation's departments of motor vehicles, the heads of which are political appointees, issued a report that made a series of recommendations as to how enhance driver's license administration and identity security. The prominence and influence that AAMVA has traditionally had on this issue is reflected in the fact that when predecessor legislative efforts to REAL ID were considered and then enacted, AAMVA was specifically mentioned in the legislation as a necessary entity to consult with the federal government on the issue of developing standards for, and enhancing the integrity of state licenses and identification documents. AAMVA continues to serve as a liaison between the state DMVs and DHS in issues related to the implementation of REAL ID.

³²⁸ National Governor's Association, "National Governor's Association Statement on Passage of REAL ID," May 12, 2005, http://www.nga.org/cms/home/news-room/news-releases/page_2005/col2-content/main-content-list/title_nga-statement-on-passage-of-real-id.html.

³²⁹ National Conference of State Legislatures, "The REAL ID: State Legislative Activity in Opposition to REAL ID," June 2012, <http://www.ncsl.org/documents/standcomm/sctran/REALIDComplianceReport.pdf>.

B. SOME STATES COMPLIED

Notwithstanding the very vocal and direct action in opposition to REAL ID, the majority of states have made progress on its implementation.³³⁰ The REAL ID regulations have a complicated method of gauging compliance by the states. The regulation established the concept of “material compliance” with the REAL ID requirements by which states’ progress is measured against 18 benchmarks that correspond to the regulatory requirements. The concept was developed as a way to “recognize and reward” states for making significant progress toward meeting the full regulatory requirements.³³¹

Congress required the DHS Office of Policy to submit a report, addressing, among other things, the progress of each state in implementing the REAL ID Act’s requirements.³³² That report was submitted to Congress on August 28, 2012. It reflected that 21 states would meet, or had committed to meet, all 18 material compliance benchmarks by January 15, 2013, with an additional five states committing to meet all benchmarks, but indicating that they would not meet the January 15, 2013 deadline.³³³ Two types of grants, FY 2008 REAL ID Demonstration Grants, and FY 2009 Driver’s License Security Grant Program, grants from the Federal Emergency Management Agency (FEMA), required the states to submit status reports on their efforts to meet 15 of the 18 material compliance benchmarks.³³⁴

³³⁰ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, ii, (For purposes of REAL ID and the report, the word state encompasses the 56 jurisdictions covered by the REAL ID Act, and thus, includes the 50 states, the District of Columbia, and the U.S. territories of Puerto Rico, the Virgin Islands, Guam, American Samoa, and Commonwealth of the Northern Marianas).

³³¹ *Ibid.*, 4.

³³² Senate Committee on Appropriations, *Senate Report 112–74*, September 7, 2011, 11.

³³³ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 9.

³³⁴ *Ibid.*, 6.

C. SOME STATES SOUGHT ALTERNATIVES TO REAL ID

NCLS is a bipartisan organization established in 1975 to support, defend, and strengthen state legislatures.³³⁵ That organization has been generally opposed to REAL ID, and on August 15, 2013, it issued the following policy statement as one of the annual policies adopted by the NCSL Standing Committee on Natural Resources and Infrastructure.

NCSL urges Congress and the administration to continue to work with NCSL and its members on alternatives to the REAL ID. NCSL supports efforts to extend existing deadlines until obstacles to implementation are addressed. In addition, NCSL supports the use of waivers by the Secretary of the Department of Homeland Security, for states that have adopted other forms of compatible identification. NCSL urges Congress and the Administration to work with NCSL and its members to adjust Title II of the REAL ID Act and develop solutions in conjunction with NCSL that recognize national security but do not impede the sovereignty of state licenses or place a federal agency or agent as a permanent and ongoing authority for determining state license uses and requirements.³³⁶

The NGA also spoke out in favor of alternatives to REAL ID. While continuing to support the need for secure driver's license and identification documents issued by the states, the NGA nonetheless, tried to persuade Congress and the administration to pass legislation that would, according to the NGA, give states more flexibility to address the issue, provide funding for implementation and greater privacy protections, and which would relieve them from using verification systems not in place.³³⁷

D. CHAPTER CONCLUSION

It is perhaps not an understatement to say that the states, and the organizations that represent their interests, have not been enthusiastic supporters of REAL ID. While 9/11 brought into full focus the problems that existed in the state system of issuing

³³⁵ National Conference of State Legislatures, *Resources for State Legislators and Legislatures About NCSL*, n.d.

³³⁶ National Conference of State Legislatures, "NCSL IN DC, Task Forces, Policies Natural Resources and Infrastructure," accessed December 15, 2013, [http://www.ncsl.org/ncsl-in-dc/task-forces/policies-natural-resources-and-infrastructure.aspx#real id](http://www.ncsl.org/ncsl-in-dc/task-forces/policies-natural-resources-and-infrastructure.aspx#real%20id).

³³⁷ Governor James H. Douglas and Governor Joe Manchin III, *National Governor's Association Letter to Congress Urging Enactment of PASS ID Legislation*, November 18, 2009.

identification documents, the states did not support the attendant costs and loss of autonomy they felt REAL ID represented. Nevertheless, the reaction of states has varied with most states moving to implement REAL ID, by taking advantage of grant programs and other available resources. However, a determined group of states has been openly hostile to the law and has taken measures available to them through the passage of laws at the state level to directly prohibit compliance with REAL ID, or at least, express disagreement with REAL ID, and an intention not to comply with the law.

Whether the states opposing REAL ID will persist in that opposition as DHS begins its phased enforcement of REAL ID requirements, remains to be seen. If any do continue to reject compliance with REAL ID, it is probable that the result will be litigation by a state or group of states seeking to strike down REAL ID as being in violation of the Constitution and an unfunded mandate. As will be discussed, DHS should seek to avoid such a confrontation with the states, by taking a variety of measures to appeal to the states and their citizens about the importance of REAL ID. One of those benefits relates to the increasing, and increasingly recognized problem of document fraud, and especially identity theft, which is the subject of the next chapter.

X. DOCUMENT FRAUD AND IDENTITY THEFT

On January 16, 2008, the *Record* newspaper of Bergen County, New Jersey published an editorial by then DHS Secretary Michael Chertoff. In that editorial, Secretary Chertoff addressed concerns, among them privacy concerns, related to the implementation of REAL ID.³³⁸ Among the primary reasons he urged full implementation of the law, was to address the problem of identity theft.

Your privacy truly is at stake in the REAL ID debate. But in my view, it's the opponents of secure identification who pose the greatest risk. Without REAL ID, you are far more likely to endure one of the worst privacy violations - having your identity stolen.³³⁹

The problem of insecure documents, including driver's licenses, represents a vulnerability being exploited by individuals and criminal organizations, and contributes to the growing and extremely costly problem of identity fraud, which encompasses identity theft. The CRS distinguishes the two by describing identity fraud as “the umbrella term that refers to a number of crimes involving the use of false identification—though not necessarily a means of identification belonging to another person.”³⁴⁰ Identity theft is “the specific form of identity fraud that involves using the personally identifiable information belonging to another person.”³⁴¹

Document fraud is of particular relevance to discussions surrounding REAL ID. Identity theft often manifests itself in the taking of personally identifiable documents to create fake or counterfeit birth certificates, licenses, and Social Security cards. These documents, in turn, can be used to obtain government benefits using the victim's name, as well as allow unauthorized aliens to remain in the United States and obtain employment. In addition, and as has been illustrated in the past, identity theft can

³³⁸ The Record, “The REAL ID Solution: Are You Who You Say You Are?” January 16, 2008, LexisNexis Academic.

³³⁹ Ibid.

³⁴⁰ Finklea, *Identity Theft: Trends and Issues*, 3.

³⁴¹ Ibid.

facilitate terrorism.³⁴² The identity fraud and theft problem has manifested itself in a variety of ways, which have federal officials alarmed, and serve to emphasize why the problem of breeder documents, including insecure identity documents like driver's licenses, are exacerbating the problems.

Identity fraud and identity theft are recognized as threats to national security, individual security, and institutional security, such as banking, healthcare and commercial institutions.³⁴³ Identity theft is also widely recognized as an international problem, whose objectives are often the acquisition of government services and documents. Stolen identities are used to access government benefits, health services, tax refunds, and obtain driver's licenses, passports, and other forms of government documents.³⁴⁴ Driver's license related identity fraud is an especially pernicious problem because perpetrators often "use drivers' license information to engage in other fraudulent activity and take advantage of the widespread use of drivers' licenses for authentication purposes."³⁴⁵ It is also seen as a problem of growing concern in terms of the influence of organized crime groups both domestic and international.³⁴⁶

A. THE SCOPE OF THE IDENTITY THEFT PROBLEM IN THE UNITED STATES

In 2012, 16.6 million people, or approximately 7% of all persons in the United States age 16 or older, were victims of identity theft.³⁴⁷ The Identity Theft Supplement (ITS) for 2012, a part of the National Crime Victimization Survey (NCVS), also estimated that direct and indirect losses from identity theft in 2012 totaled \$24.7

³⁴² Finklea, *Identity Theft: Trends and Issues*, 19–20. As noted in the CRS report, former Attorney General John Ashcroft noted that an Algerian national had stolen the identities of 21 members of a health club, and transferred the identities to an individual later convicted of the plot to bomb LAX in 1999.

³⁴³ Finklea, *Identity Theft: Trends and Issues*.

³⁴⁴ UNODC, "Handbook on Identity-Related Crime 2011," accessed August 22, 2013, <http://www.unodc.org/unodc/en/organized-crime/tools-and-publications.html>, 118.

³⁴⁵ *Ibid.*, 119.

³⁴⁶ *Ibid.*

³⁴⁷ Erika Harrell and Lynn Langton, "Victims of Identity Theft, 2012," *Bureau of Justice Statistics*, December 2013, <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.

billion.³⁴⁸ To put the scale of the losses from identity theft in perspective, the losses in 2012 from all other property crimes (burglary, motor vehicle theft, and theft) totaled \$14 billion. Thus, as noted in the ITS, identity theft losses exceeded those from burglaries and theft by more than four times, and losses from motor vehicle thefts by more than eight times.³⁴⁹

The problem of identity theft also appears to be growing. The 2008 ITS for Victims of Identity Theft estimated that in the preceding two years, 11.7 million persons, representing 5% of the U.S. population over the age of 16, had been victims of identity theft, with a corresponding direct and indirect losses estimated to be 17.3 billion over that two-year period.³⁵⁰ Some uncertainty exists as to whether in more recent years the occurrence of identity theft is increasing, decreasing, or changing in significant ways. Despite growing concerns about identity theft, between FY 2009 and FY 2010, the number of identity theft cases and associated prosecutions decreased relative to FY 2008. Varying explanations for this decrease have been posited, including speculation that that fewer incidents have occurred, or that fewer law enforcement resources are being devoted to the issue. However, some research indicates that the number of individuals victimized has increased but that the perpetrators are better able to evade law enforcement, that law enforcement resources dedicated to the issue have decreased, or that the prosecutions have shifted to address cases of aggravated identity theft.³⁵¹ It is worth noting that estimates of identity theft losses are compiled by different sources and some variation

³⁴⁸ Harrell and Lynn Langton, "Victims of Identity Theft, 2012."

³⁴⁹ Ibid.

³⁵⁰ Lynn Langton and Michael Planty, *Victims of Identity Theft, 2008*, National Crime Victimization Survey, Bureau of Justice Statistics, December 2010.

³⁵¹ Finklea, *Identity Theft: Trends and Issues*, 16–17 Aggravated identity theft refers to the form of the crime introduced by the Identity Theft Penalty Enhancement Act that brings enhanced penalties under the law when the offense is committed in connection with other federal offenses. (Public Law 108–275). The offenses include theft of public property, thefts by bank officers or employees, theft from employee benefit plans, theft of Social Security and Medicare benefits, several immigration related fraud offenses, and specific violations related to terrorism.

may occur between the sources.³⁵² Nevertheless, the estimated costs of identity theft are substantial.

One area in which identity theft is clearly increasing is that of identity theft used to obtain tax refunds fraudulently. Government officials note that close to \$3.6 billion in fraudulent tax refunds were obtained in tax year 2011.³⁵³ According to tax officials, the problem has grown exponentially in the last three years, which caused nearly 1,500 investigations to be launched last year, up from just 276 in FY 2011.³⁵⁴ A particularly troublesome issue associated with identity theft is seen in the weaknesses being exploited in the ITINs. It is now known that the application process for ITINs is subject to fraud. State driver's license bureaus are allowing ITINs to be used by illegal aliens to obtain driver's licenses even though the ITINs are only to be used only as a taxpayer identification number and not as proof of identity.³⁵⁵ Since the majority of readers are likely unfamiliar with the ITIN number, some background may be helpful.

Individuals employed in the United States are required to have a valid SSN for employment.³⁵⁶ The SSN is required to be used to file tax returns, to report income, and for record-keeping purposes. Persons required to file tax returns are required to include an identifying number. That number included on the tax returns is known as the taxpayer identification number.³⁵⁷ For most people, the number included is the SSN. In 1996, the Internal Revenue Service (IRS) created the ITIN to provide tax identification numbers to people who do not have or are not eligible to obtain an SSN. Individuals receiving an

³⁵² For example, the CRS cites to a source that put the estimated cost of identity theft to Americans in 2010 at \$37 billion. This estimate, citing Javelin Strategy & Research, 2011 Fraud Survey Report: Consumer Version, February 2011, would seem to indicate, when compared to the BJS estimate for 2012 that identity theft actually decreased in 2012.

³⁵³ Matt Zapotosky, "IRS Tax Refund Thieves Increasingly Use Stolen Identities to Divert Money to Themselves," *The Washington Post*, sec. Local, February 19, 2014, http://www.washingtonpost.com/local/crime/irs-tax-refund-thieves-increasingly-use-stolen-identities-to-divert-money-to-themselves/2014/02/18/4bd7f4cc-7ed0-11e3-9556-4a4bf7bcbd84_story.html?hpid=z4.

³⁵⁴ *Ibid.*

³⁵⁵ Treasury Inspector General for Tax Administration, *Substantial Changes Are Needed to the Individual Taxpayer Identification Number Program to Detect Fraudulent Applications*, 29.

³⁵⁶ *Ibid.*, 2.

³⁵⁷ Treasury Inspector General for Tax Administration, *Substantial Changes Are Needed to the Individual Taxpayer Identification Number Program to Detect Fraudulent Applications*.

ITIN should be either someone residing in the United States but not authorized to work, or a nonresident of the United States.³⁵⁸

In July 2012, the Treasury Department's Inspector General for Tax Administration (TIGTA) issued a report regarding the absence of adequate measures to prevent fraud in the acquisition of ITINs. The report, launched in response to congressional inquiries based on whistleblower complaints, uncovered a number of management failures that had gutted anti-fraud measures in the ITIN process. It also shed light on the pernicious problem of fraud in the ITIN application process and why it matters. Perpetrators of fraud are exploiting vulnerabilities in the program, which serves to undermine a substantial tax related program that puts revenues at risk through fraudulent refunds or credits.

The TIGTA report demonstrates that between October 2007 to April 2010, the Wage and Investment Division, which administers the ITIN program, identified tens of thousands of fraudulent ITIN tax returns with erroneous tax refunds totaling more than \$43 million dollars.³⁵⁹ TIGTA also determined that inadequate procedures were in place to verify each applicant's identity and foreign status, and recited various recommendations made in the past that had not been followed, and existing processes in place that created identity theft vulnerabilities.

TIGTA also noted that what had been intended as a number to be used for filing tax returns for people ineligible for a Social Security card, was increasingly being used as a federal identification number for non-tax purposes. TIGTA noted that the use of the ITIN for various non-tax purposes increased the need for adequate processes to ensure that only eligible individuals receive the ITINs.³⁶⁰ The fraudulent acquisition and use of ITINs, and the improper acceptance of ITINs as proof of identification by states when issuing identification documents, highlight the vulnerabilities, to both the financial system, and the integrity of the identity document issuance process by states. REAL ID

³⁵⁸ Treasury Inspector General for Tax Administration, *Substantial Changes Are Needed to the Individual Taxpayer Identification Number Program to Detect Fraudulent Applications*, 2.

³⁵⁹ *Ibid.*, 13.

³⁶⁰ *Ibid.*, 29.

would have additional benefits in stemming these types of activities by helping to ensure that the identity documents presented to acquire an ITIN were reliable, and that the identity documents issued by states are issued under more rigorous processing requirements than currently exist, and which, are clearly being exploited.

In addition to the specific ITIN fraud, the TIGTA has also examined the issue of the impact of identity theft in the tax administration system in general. It has estimated that for processing year 2011, the IRS identified 2.2 million tax returns as fraudulent. Of those, approximately 940,000 tax returns involved identity theft, and were associated with \$6.5 billion in associated fraudulent tax refunds involving identity theft.³⁶¹

While the impact of identity theft on the fraud is associated with tax administration, it is also the case that the issue of identity theft and document fraud has a nexus to illegal immigration and facilitates the stay of persons illegally in the United States. Illegal immigrants or others may use stolen identities to obtain employment and then disappear without paying taxes that leaves the victim with a large outstanding tax bill. One U.S. taxpayer was reportedly faced with a \$1 million back-tax bill, even though she was a stay-at-home mother. An investigation later found that 218 illegal immigrants were using her SSN. From 2002 through 2005, multiple identity criminals used the name and SSN of a Mexican-American factory worker to get jobs in Kansas, Texas and New Jersey. The victim had to deal with repeated allegations of under-reported income and long delays in receiving tax refunds owed to him.³⁶²

Finally, and potentially most significant from the standpoint of national security, is the problem of identity fraud and theft in connection with the acquisition of U.S. passports. In July 2010, the GAO testified before Congress in connection with its efforts to conduct undercover testing to identify vulnerabilities in the Department of State's

³⁶¹ *Testimony of the Honorable J. Russell George Treasury Inspector General for Tax Administration: Identity Theft and Tax Fraud* (Washington, DC, 2012).

³⁶² "Handbook on Identity-Related Crime 2011," 119 citing to Kevin McCoy, "Identity Thieves Tax the System," *USA Today*, April 10, 2008.

(DOS) passport issuance processes.³⁶³ This testimony was a follow-up to a 2009 GAO audit.³⁶⁴ This type of vulnerability is extremely significant given the desirability of and privileges afforded to holders of U.S. passports. As the GAO noted, people who seek to acquire U.S. passports through fraud are typically doing so to conceal involvement with serious crimes, such as terrorism, narcotics trafficking, money laundering, or murder. The GAO concluded that DOS remained vulnerable to fraud as the results of its testing showed that five of seven U.S. passports were issued, despite the existence of multiple indicators of fraud or identity theft in each of the applications.

B. FEDERAL RECOGNITION OF AND EFFORTS TO ADDRESS DOCUMENT FRAUD AND IDENTITY THEFT

The terrorist attacks of 9/11 brought increased attention to those issues, but the federal government has been aware of the problem of document fraud and its facilitation of false identities and identity theft for some time, and has sought to identify and tackle a myriad of issues to address identity theft. Interestingly, identity theft itself was not made a federal crime until 1998.³⁶⁵ With the increase in Internet use and associated identity theft crimes, calls were made for more effective laws to address the issue, which resulted in a series of laws enacted between 1998 and 2008.³⁶⁶ The 1998 legislation known as the Identity Theft and Assumption Deterrence Act became effective in October 1998. The law established identity theft as a federal crime, and charged the Federal Trade Commission with the responsibility of accepting complaints from victims, sharing information with federal, state and local agencies, and assisting victims of identity theft.³⁶⁷

³⁶³ Statement of George Kutz, Managing Director, Forensic Audits and Special Investigations, General Accountability Office, *Hearing Before the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary* (July 29, 2010).

³⁶⁴ *Ibid.*

³⁶⁵ Finklea, *Identity Theft: Trends and Issues*, 3.

³⁶⁶ *Ibid.*, 3–4.

³⁶⁷ *Identity Theft and Assumption Deterrence Act*, Public Law 105–318, 112 Stat. 3007, 1998, <http://www.gpo.gov/fdsys/pkg/PLAW-105publ318/html/PLAW-105publ318.htm>.

Some assert that the problem of identity theft can be curtailed through greater efforts to secure the identification document issuance process.³⁶⁸ The call for improved verification procedures and improvements to the issuance process of driver's licenses and identity cards has been longstanding and repeated. The GAO offered testimony on the issue of identity document vulnerabilities in September 2003, and shortly thereafter on September 15, 2003, it issued a report specifically examining the issue of identity document vulnerabilities and ways to improve the verification and issuance process.

On September 9, 2003, the General Accountability Office (GAO, then known as the General Accounting Office), provided testimony before the Senate Committee on Finance. In that testimony, GAO's Managing Director of the Office of Investigations testified about the various GAO studies, which demonstrated the security vulnerabilities that existed due to the ease with which counterfeit identification could be produced and used to create fraudulent identities.³⁶⁹ The vulnerabilities identified were associated with a variety of critical functions and activities, such as the following.

- Firearms purchased from federal firearms licensees using bogus identification³⁷⁰
- Breaches at federal agencies and airports³⁷¹
- Purchase of firearms using a counterfeit federal firearms license³⁷²
- Counterfeit documents used to enter the United States from certain western hemisphere countries not detected³⁷³
- SSNs: Ensuring the Integrity of the SSN³⁷⁴

³⁶⁸ U.S. Government Accountability Office, *Driver's License Security*.

³⁶⁹ U.S. Government Accountability Office, *Testimony Before the Senate Committee on Finance, Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*, (2003).

³⁷⁰ U.S. Government Accountability Office, *Firearms: Purchased from Federal Firearms Licensees Using Bogus Identification*, (2001).

³⁷¹ U.S. Government Accountability Office, *Security: Breaches at Federal Agencies and Airports*, (2000); U.S. Government Accountability Office, *Security Breaches at Federal Buildings in Atlanta, Georgia*, (2002).

³⁷² U.S. Government Accountability Office, *Counterfeit Documents Used to Enter the United States from Certain Western Hemisphere Countries Not Detected*, (2003).

³⁷³ U.S. Government Accountability Office, *Purchase of Firearms Using a Counterfeit Federal Firearms License*, (2002).

³⁷⁴ U.S. Government Accountability Office, *Social Security Numbers: Ensuring the Integrity of the SSN*, (2003).

The testimony offered by the GAO in September 2003 to the Finance Committee noted three overall findings from its special investigations: 1) government officials generally did not recognize counterfeit documents when presented, 2) some government officials failed to follow security procedures and seemed unaware of the possibility of identity fraud, and 3) identity verification procedures were inadequate.³⁷⁵ The recommended solutions included improving verification procedures to minimize vulnerabilities posed by such documents.³⁷⁶

The GAO explained the problem the problem faced by the state DMVs as follows.

Driver licensing agencies face the challenge of determining whether the identity documents individuals provide (1) are authentic and contain information that agrees with the issuing agency's records and (2) actually belong to the person presenting them.³⁷⁷

That GAO report examined two principal vulnerabilities in the driver's license application and issuance process. One was the need to verify SSN information presented by driver's license applicants, by cross checking that information with the SSA, using a service provided by SSA to state DMVs for that purpose.³⁷⁸ The second vulnerability was that states lacked a systematic means to exchange driver's license information. This deficiency, in turn, made states susceptible to issuing driver's licenses to individuals by accepting false out-of-state licenses, and by issuing licenses to individuals using the identity information of others and presenting it as their own.³⁷⁹ The report noted that GAO's own investigators were able to obtain driver's licenses in states whose practices they examined by using counterfeit out-of state driver's licenses, other fraudulent documents, and the SSNs of deceased persons.³⁸⁰

³⁷⁵ U.S. Government Accountability Office, *Testimony Before the Senate Committee on Finance, Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*, 1.

³⁷⁶ *Ibid.*, 4.

³⁷⁷ U.S. Government Accountability Office, *Social Security Numbers: Increased SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification*, (2003), 5.

³⁷⁸ *Ibid.*

³⁷⁹ *Ibid.*, 16.

³⁸⁰ *Ibid.*, 3.

According to the GAO, the use of the SSN verification service varied widely, and inadequate and inconsistent verification measures resulted in the ability of perpetrators of fraud to obtain state issued driver's licenses by presenting fraudulent documents and SSN information related to deceased individuals.³⁸¹ Aside from SSA related recommendations, the report—issued a year-and-a-half before the passage of REAL ID—also made recommendations for consideration by Congress related to the ability of licensing bureau employees to have access to means of verifying information presented, and the ability of states to exchange driver's license information.

The report discussed various measures individual states were taking to verify information presented to them using private vendors or through negotiated agreements with DHS to access data to verify immigration information. Nevertheless, the GAO found that states lacked a systematic means to exchange information on all drivers nationwide, which the GAO found limited the states' ability to deter fraud and identity theft.³⁸²

The problem this posed, as identified to the GAO was as follows.

Numerous officials in the states we visited told us that having a more efficient means of electronic interstate communications, that included the electronic transfer of identity information such as digital photographs and signatures, would improve the integrity of their licensing process. Officials in the states we visited were particularly concerned about individuals using licenses issued by other states as identity documents and their inability to quickly query all states' databases to corroborate key information. As a result, states are limited in their ability to determine whether other states' identity documents are authentic or to identify multiple individuals using the same personal identifying information in other states.³⁸³

Among the measures taken to address identity theft was the passage of the REAL ID Act, which was intended to improve the accuracy, and reliability of identification documents that state governments issue.³⁸⁴ In addition, in 2006, President Bush issued an Executive

³⁸¹ U.S. Government Accountability Office, *Social Security Numbers: Increased SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification*, 15.

³⁸² *Ibid.*, 20.

³⁸³ *Ibid.*, 21.

³⁸⁴ The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007, 43.

Order 13402, which, among other things, established the President's Task Force on Identity Theft. The task force developed a strategic plan for addressing identity theft.

C. CHAPTER CONCLUSION

The discussion of these various reports highlights the prevalence of identity theft abusing such programs by those who seek to steal, and hide their true identities. These activities pose significant risks to the integrity of the programs being exploited, and incur huge costs for the government, and the individuals whose identities are stolen or who otherwise are harmed by these activities. These activities are only some of the activities being perpetrated using identity theft and fraud, and highlight those that represent government programs. An entirely different sphere of identity theft poses problem for non-governmental programs, such as commercial transactions, and other private interactions.

As early as 2003, and reiterated as recently as its report in 2012, the GAO has identified a need for concerted action led by the federal government to improve the exchange of driver record data among the states to curtail the problems associated with fraudulent documents, noting:

We recognize that potential barriers related to system's design, funding, privacy rights, and states' willingness to use such a tool have yet to be fully resolved. However, given the potential economic and national security implications associated with identity theft at the point of driver licensing, sustained leadership at the federal level could be the catalyst for needed change.

In light of the homeland security implications associated with states' inability to systematically exchange driver license identity information and the need for sustained leadership in this area, the Congress, in partnership with the states, should consider authorizing the development of a national data sharing system for driver records.³⁸⁵

The GAO's recommendation regarding the exchange of state information, which it called, "a matter for congressional consideration" was, along with efforts by the AAMVA, and the 9/11 Commission's recommendation regarding federal standards, were

³⁸⁵ U.S. Government Accountability Office, *Social Security Numbers: Increased SSN Verification and Exchange of States' Driver Records Would Enhance Identity Verification*, 23.

motivators for REAL ID. However, as has been discussed, the legislation did not establish a nationwide registry; yet, it did require and facilitate the sharing of records among the states.

While REAL ID will not eliminate identity theft and fraud, its requirements create a more secure environment for identity document issuance and verification.

XI. STATE CASE STUDIES

This chapter presents case studies of three categories of states that demonstrate the range of compliance or non-compliance by the states with REAL ID standards, to include states that complied early, states that have worked steadily toward compliance despite obstacles, and states that have defied compliance. The chapter examines, from publicly available information, factors that contributed to the states' current compliance status with REAL ID. Delaware was an early adopter of the REAL ID standards and was in the first group of states found by DHS to be fully compliant with REAL ID. New Jersey is a state that has made steady and incremental progress toward REAL ID. It was on the cusp of compliance in October 2012, but external factors intervened and halted its progress. Finally, Maine represents the handful of holdout states that have defied DHS and have not only asserted its intention to not comply with REAL ID, but has taken affirmative action in the form of passing state laws to prohibit compliance. The REAL ID experience of each state is instructive as to the factors that contributed to each state's approach and compliance status. Those experiences are presented to identify issues that have arisen, identify lessons learned, and flag issues for DHS attention that may allow it to tailor its approach to such states and facilitate and nudge them toward full compliance.

A. DELAWARE

1. Early REAL ID Efforts by Delaware

The State of Delaware's efforts are examined first. Delaware has proven to be one of the states that has undertaken to implement the REAL ID provisions fully, and has proven to be a leader in those efforts, having been among the first group of states to be found in full compliance with the provisions. Although it was an early adopter, Delaware had been an early advocate for the states in terms of their concerns with REAL ID. It had raised those concerns to Congress, asking that states be relieved from fully implementing REAL ID provisions until the following concerns were addressed.

- States were provided with funding
- The necessary databases were established to support state efforts

- Workable deadlines were identified
- States were provided with flexibility to assist them in complying with the federal mandate and lessen the “drastic impacts” on their citizens³⁸⁶

2. Best Practices/Efforts by Delaware to Nudge Public Compliance

An examination of Delaware’s DMV website demonstrates that Delaware has undertaken clear efforts to inform the public and project the image of a secure driver’s license as something beneficial both to the public and individuals. For example, the logo on the DMV website page that discusses the REAL ID requirements is labeled, iDelaware Card with the words “iD” and “Card” appearing in red color font, thus reading, “iD Card.” The logo contains the slogan, “A Lifetime of Security” and contains the image of a Delaware driver’s license secured by a padlock, which further increased the image of security (see Figure 11).



Figure 11. Image and Logo of a Delaware’s Driver’s License³⁸⁷

Further, the Delaware DMV website page addressing REAL ID is user-friendly, laid out with a listing of frequently asked questions, and with a section designed to directly address misconceptions about REAL ID, entitled, “Federal Identification Standards Facts and Myths,” which lists a variety of things that the REAL ID compliant license “does not” do. Interestingly, among the myths it seeks to debunk is the notion that

³⁸⁶ Governor Ruth Ann Minner, *Will REAL ID Actually Make Us Safer: Privacy and Civil Liberties Hearing May 2007* (Washington, DC, 2007).

³⁸⁷ State of Delaware Division of Motor Vehicles, “Graduated Driver License,” accessed July 9, 2013, http://www.dmv.de.gov/services/driver_services/drivers_license/dr_lic_secure_dl_get_started.shtml.

the secure licensing process does not “control, restrict, or affect” gun sales.³⁸⁸ The website’s main page on secure ID also has easy to navigate buttons labeled as follows.

- Get Started
- Document Guide
- Video
- Brochure
- FAQ

The site also contains a link to the relevant provision of Delaware Administrative Code, 2217 *Driver License and Identification Card Application Procedures for Delaware Compliant and Delaware Non-Compliant Identification Documents*, which sets forth Delaware’s detailed administrative code provisions relating to compliant and non-compliant driver licenses and identification cards.

In addition to the information contained on the DMV site, Delaware has also taken advantage of other commonly accessed state resources to disseminate information to the public about REAL ID. For example, it has responded to inquiries related to REAL ID on the Delaware Division of Libraries’ site where it maintains a blog, and has posted a response to an inquiry related to REAL ID.³⁸⁹ The state has also provided a high degree of transparency and communication to the public, by issuing a press release in April 2009, and announcing its intention to begin issuing its secure driver’s license and ID card system later that year to comply with REAL ID.³⁹⁰ Delaware’s press release, issued seven months before it anticipated beginning the new process for secure driver’s licenses, noted that it had awarded a contract for the program, and named the company that had been awarded the contract.³⁹¹

³⁸⁸ State of Delaware Division of Motor Vehicles, “Graduated Driver License.”

³⁸⁹ Division of Libraries’ Blog, “Q: ‘What Is a Federally Compliant Delaware Driver’s License (and ID)?,’” accessed December 23, 2013, <http://library.blogs.delaware.gov/2012/10/07/federally-compliant-de-drivers-license/>.

³⁹⁰ Delaware Department of Transportation, “Press Release: DMV Announces New Secure Driver License and Identification Card System,” April 13, 2009, <http://www.del.dot.gov/public.ejs?command=PublicNewsDisplay&id=3324>.

³⁹¹ Ibid.

The press release also contained a fact sheet, and within that fact sheet it noted that in order to protect its residents against identity theft, it was also implementing a facial recognition system. This is something not required by REAL ID, but which demonstrates the seriousness with which Delaware has approached the issue of secure identification documents.

3. Leadership Matters: DMV Chief, Jennifer Cohan

One of the major reasons that Delaware has been a leader in REAL ID compliance has to do with the efforts of Jennifer L. Cohan, Delaware's Director of the Division of Motor Vehicles, who has been in the position since 2007. In Delaware, the Director of the DMV is not a political appointee. The current governor, Jack Markell, is a Democrat elected in 2008. The DMV falls within the DOT, a cabinet department requiring state Senate confirmation, led by Secretary Shailen P. Bhatt.³⁹² The DMV is an agency under DelDOT, and lists as its first key objective:

Issue secure and accurate driver license and identification cards while ensuring those individuals obtaining Delaware credentials are representing their identity accurately, are in the country legally, meet all the requirements for obtaining driving privileges and have demonstrated their Delaware residency.³⁹³

Prior to assuming leadership of the DMV, Cohan has held a variety of other positions within the DMV and within the State of Delaware.³⁹⁴ She has been a leader on issues associated with secure driver licenses and identity cards, having appeared as a speaker before AAMVA and at think tank events, such as a program on REAL ID hosted by the Heritage Foundation. Ms. Cohan participated in a panel discussion on REAL ID held at the Heritage Foundation in Washington, DC, and co-sponsored by the Coalition for Secure Driver's Licenses (CSDL). Ms. Cohan emphasized that Delaware felt that

³⁹² State of Delaware, "Delaware Department of Transportation—Secretary," accessed January 31, 2014, <http://www.deldot.gov/home/secretary/>.

³⁹³ State of Delaware, "Delaware Department of Transportation—Divisions," accessed July 9, 2013, <http://www.deldot.gov/home/divisions/>.

³⁹⁴ State of Delaware, DelDOT Newsroom, *Press Release: The American Association of Motor Vehicle Administrators Welcomes Delaware Director of DMV as Chairwoman of the International Board of Directors*, September 4, 2013.

implementing the law was the right thing to do in terms of identity protection for its citizens.³⁹⁵ She noted the effectiveness of Delaware's REAL ID implementation efforts in addressing identity issues, observing that in examining its driver's license records as part of the compliance process, it identified over 1,300 imposters as having obtained driver's licenses in recent years and that "most of these people had on average between nine to twenty different identities. Some of those people were actually in major crime syndicates."³⁹⁶ She also touted the fraud deterrence as a result of Delaware's compliance efforts noting that previously the state would generally identify three to four weekly attempts to obtain documents fraudulently. After it began its compliance efforts, it only saw six attempts in the past year.³⁹⁷

AS DMV Director, Ms. Cohan has taken a very pragmatic approach to the implementation of REAL ID, explaining in an interview why Delaware chose to pursue early implementation when the state had several years to comply with the law.

The reason we started now is because we don't have the resources to have everyone come in at one time. If we start now everyone has five years to come in during their normal renewal periods. When it's your time, we'll send you a letter telling you everything you have to bring. It's completely optional for our customers, they don't have to get one, but if they don't they have to use a passport to get on an airplane or to get in federal buildings. And it's definitely cheaper for our customers to do it this way.³⁹⁸

Delaware also took advantage of the federal funding provided to states to help it make the transition to more secure identity documents. Cohan stated that Delaware had received \$1 million dollars from the federal government and had used that money to upgrade its computer system, which facilitated the issuance of more secure documents.³⁹⁹ While initially it would be more of a hassle for residents because of the need to present an

³⁹⁵ The Heritage Foundation, "REAL ID Realities: Perspectives on the Future of the REAL ID Program," accessed February 1, 2014, <http://www.heritage.org/events/2013/01/real-id>.

³⁹⁶ Ibid.

³⁹⁷ Ibid.

³⁹⁸ Doug Denison, "Newsmaker Q&A: Jennifer Cohan, Director of the Delaware Division of Motor Vehicles," *Dover Post*, August 24, 2010, <http://www.doverpost.com/apps/pbcs.dll/article?avis=DE>.

³⁹⁹ Doug Denison, "Delaware DMV Unveils New Secure ID Cards," *Middletown Transcript*, June 16, 2010, <http://www.middletowntranscript.com/apps/pbcs.dll/article?avis=DE>.

original birth certificate or passport along with a social security card and evidence of state residence, future renewals would be aided by the computer system, and the use of facial recognition technology to retrieve previous record would make renewals a more efficient for residents.⁴⁰⁰

4. Delaware's Efforts and Leadership Have Been Recognized

The non-profit group CSDL recognized Delaware DMV efforts for a secure driver's license on May 29, 2012, when its employees received the organization's "Identity Security Award" at a presentation made by CSDL's President, and attended by the Delaware's Governor, DOT Secretary and DMV Chief.⁴⁰¹ Delaware was the 9th state to have been presented with the award.⁴⁰² Some background on CSDL is appropriate given the role this organization has played in promoting state DMV practices that address document security and measures to prevent identity theft since its founding in November of 2001. As noted in the organization's website:

In the immediate aftermath of the September 11, 2001 terrorist attacks in New York City and Washington, DC, it was revealed that 18 of the 19 terrorists involved in the 9/11 attacks held over thirty valid driver's licenses and ID cards issued by five states. The reason that the terrorists had obtained so many state IDs was to escape detection by airport security systems that use passport data to check foreign visitors against federal watch lists.⁴⁰³

The organization was clearly motivated by the 9/11 attacks, and its concern with the "apparent indifference by state and federal officials to this security vulnerability."⁴⁰⁴ The organization describes itself as a non-partisan, not for profit entity, interested in crime prevention. Its objective is to raise public awareness about states with weak identity document issuance systems that pose risks of terrorism and a variety of crimes

⁴⁰⁰ Denison, "Delaware DMV Unveils New Secure ID Cards."

⁴⁰¹ Delaware Department of Transportation, "Press Release: Division of Motor Vehicles Receives Award for Outstanding Fraud Protection of State Residents," May 29, 2012, <http://www.deldot.gov/home/newsroom/release.shtml?id=4370>.

⁴⁰² Ibid.

⁴⁰³ Coalition for a Secure Driver's License, "About Us," accessed February 13, 2014, <http://www.secure-license.org/about-us>.

⁴⁰⁴ Ibid.

and to highlight efforts of states relative to their efforts on REAL ID. It also notes that it has been a vocal supporter of REAL ID and urges states to improve the security of their state issued driver's licenses.⁴⁰⁵ One of its major activities has been to examine the practices of the state motor vehicle administrators and how they are implementing REAL ID, engage with the states, and highlight their efforts regarding secure identity document issuance. It includes information of this nature on its website, and it also recognizes states for their efforts at improving the security of its licensing practices.⁴⁰⁶

Ms. Cohan's influence has been recognized within the community of motor vehicle and licensing administrators. At the AAMVA's 80th Annual International Conference, held in August of 2013, Ms. Cohan was elected as the chairwoman of AAMVA's International Board of Directors.⁴⁰⁷

5. Media Coverage in Delaware

Delaware's media has not expressed open hostility toward REAL ID, such as has been the case with other states. Rather, the news outlets, at least print media, have taken a more cautious, wait and see approach. Rather than any fundamental disagreement with REAL ID, the media's coverage has focused more on inconvenience to the citizens of Delaware, as reflected in a *News Journal* editorial dated May 25, 2008, which predicted lines at DMV offices, a variety of implementation headaches, and impacts on civil liberties, even while acknowledging the terrorism-related concerns that led to the law. The editorial did not so much oppose REAL ID, as it expressed skepticism about the ability of DMV officials to implement the law effectively and affordably.

With a year and a half to go before Real ID is supposed to be ready to roll, it's time to decide if it's really possible to link up such a fail-safe system, and at what price. And will the government back up a federal security

⁴⁰⁵ Coalition for a Secure Driver's License, "About Us."

⁴⁰⁶ Ibid. Although the CSDL appears to be an important voice in discussions concerning secure driver license practices, its website is not as robust as it could be and does not appear to maintain the most current information available; in part, due to the fact that it maintains separate subscriber content.

⁴⁰⁷ State of Delaware, DelDOT Newsroom, *Press Release: The American Association of Motor Vehicle Administrators Welcomes Delaware Director of DMV as Chairwoman of the International Board of Directors*.

commitment with the right amount of money? If this is only going to be an unreliable make-work project, pull the plug.⁴⁰⁸

A year-and-a-half later, the *News Journal* observed that Delaware was one of the few states that had come into compliance with REAL ID, and had not raised objections to the law. It noted that the state's size and federal subsidies would allow the state to roll out the new, secure identification documents with relative ease, while at the same time noting with approval, the introduction of alternative legislation to REAL ID, known as PASS ID.⁴⁰⁹

Another editorial reflecting Delaware's implementation efforts was one appearing on July 24, 2010, shortly after the states' roll out of REAL ID. In that editorial, objections were not to the law itself, but rather to the states' early implementation efforts during which staffing shortages were not addressed that led to two to three hours waits at the DMV offices.⁴¹⁰ Thus, at least in Delaware, REAL ID did not experience overt hostility to the implementation efforts, and was able to overcome early skepticism about its ability to make its efforts efficient, and thus, address early editorial objections, and the criticisms.

6. Delaware Has Unique Advantages Aiding Its Implementation Efforts

While Delaware has benefitted from strong leadership on the issue of secure identification documents, it is, of course, a small state, and does not have all of the challenges of others states. For example, the DMV website indicates that it has 650,000 licensed drivers in the state, a number that is much smaller, of course, than that of many

⁴⁰⁸ The News Journal, "Real ID Has So Many Pitfalls And Not Enough Money To Back It Up," May 28, 2008, LexisNexis Academic.

⁴⁰⁹ The News Journal, "Proposed Changes in Secured ID Could Make Law More Workable," October 20, 2009, LexisNexis Academic.

⁴¹⁰ The News Journal, "DMV Must Get a Handle on Real ID to Ease Delays," July 24, 2010, LexisNexis Academic.

other states.⁴¹¹ By way of comparison, Maine, also a small state population wise, has over 1 million licensed drivers, and New Jersey has nearly 6 million drivers.⁴¹²

B. NEW JERSEY

After being on its way toward achieving compliance with REAL ID, New Jersey's implementation effort stopped in its tracks in October 2012, in the wake of litigation brought by the ACLU, which had won a temporary court order in May of that year blocking the implementation of the law on the basis of privacy concerns, and due to the court's determination that insufficient public input had been sought prior to New Jersey's implementation.⁴¹³ After extensions of the court order based on ongoing settlement discussions between the parties, New Jersey agreed that it would not take any further action to implement its roll out of Tru-ID, its name for its REAL ID compliant licenses, until it engaged in rulemaking.⁴¹⁴

1. New Jersey's Attempt to Implement REAL ID

Prior to the ACLU lawsuit, New Jersey seemed well on its way toward pursuing full implementation of REAL ID. On April 2, 2012, New Jersey announced its intention to adjust the issuance process for its driver's license and non-driver IDs to bring the state into compliance with REAL ID, beginning with document renewals in July 2012.⁴¹⁵ New Jersey's TRU-ID program, scheduled to begin May 7, 2012, was to replace New Jersey's existing renewal program, known as the 6 Point ID Verification. TRU-ID licenses would

⁴¹¹ State of Delaware, "State of Delaware Division of Motor Vehicles—About DMV," accessed July 9, 2013, <http://www.dmv.de.gov/>.

⁴¹² State of Maine, "Secretary of State Matt Dunlap Takes Oath for Third Term," accessed February 23, 2014, <http://www.maine.gov/sos/news/2009/sosthirdterm.htm>; State of New Jersey, Motor Vehicle Commission, "Chief Administrator," accessed March 2, 2014, <http://www.state.nj.us/mvc/About/ChiefAdministrator.htm>.


⁴¹³ Mike Frassinelli, "N.J. Drops Plan to Require Extra Documents to Get Driver's License," accessed September 14, 2013, http://blog.nj.com/ledgerupdates_impact/print.html?entry=/2012/10/nj_drops_plan_to_require_addit.html.

⁴¹⁴ *Ibid.*

⁴¹⁵ State of New Jersey, Motor Vehicle Commission, "Media Release: Christie Administration Announces New 'Skip the Trip' Drivers License and ID Mail Renewal Service for New Jerseyans New Process to Aid Implementation of Federal REAL ID Standards," April 2, 2012, <http://www.state.nj.us/mvc/PressReleases/archives/2012/040212.htm>.

be distinguishable by what the press release called “the federally mandated designation of a gold star” in the upper right-hand corner. The “gold star” comes from a publication created by DHS to assist states, entitled “REAL ID Mark Guidelines” (October 2008) that provided DHS recommendations for the licenses.⁴¹⁶

The following information appeared on the New Jersey DMV website regarding the changes.



TRU-ID (effective 5/7/12)

What is TRU-ID?
 TRU-ID is New Jersey's implementation of the federal REAL ID Act, which sets new standards for the issuance of driver licenses and identification cards.

The United States Department of Homeland Security has released its rules governing the implementation of the REAL ID Act.

New Jersey will begin issuing compliant driver licenses, non-driver IDs and permits at its agencies statewide beginning on May 7, 2012. The new credentials will have a single gold star or a single gold star in a circle in the upper right corner of the card as shown in the sample license example on the left.

Facts to Know...




Figure 12. New Jersey TRU-ID Information and Image of Driver's License⁴¹⁷

New Jersey's Chief Administrator of the Motor Vehicle Commission (MVC), Raymond P. Martinez, stressed that residents would not encounter major changes as the state implemented REAL ID, noting:

⁴¹⁶ Honolulu Star-Advertiser, “State Driver's Licenses, ID Cards Do Not Conform to Federal,” accessed February 16, 2014, http://www.staradvertiser.com/news/20110428_State_drivers_licenses_ID_cards_do_not_conform_to_federal_rules.html; Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 3.

⁴¹⁷ State of New Jersey, Motor Vehicle Commission, “TRU-ID,” accessed February 8, 2014, <http://www.state.nj.us/mvc/Licenses/truid.htm>.

Although the federal government has laid out new identity requirements, it's important to note that TRU-ID is not that different from the six points that we've all become accustomed to presenting. With documents like your official birth certificate, social security card and mail from your bank and utility company, you'll be able to meet the new requirements.⁴¹⁸

New Jersey was also launching an effort to renew licenses by mail, the purpose of which was to facilitate the implementation of Jersey's TRU ID program by reducing the number of persons appearing at MVC offices by postponing for four years the need for citizens to visit a MVC office in person.⁴¹⁹ New Jersey MVC officials stressed that no leeway existed in terms of compliance with the REAL ID requirements, and noted that its efforts were geared at ensuring that New Jersey residents were in possession of REAL ID compliant licenses at the time that the federal government began enforcing REAL ID. They also emphasized that the current efforts were a culmination of efforts that New Jersey had begun two years previously to enhance security features of its driver's licenses to begin its compliance with REAL ID.⁴²⁰

2. The ACLU Lawsuit

The ACLU's litigation against TRU-ID was filed in May 2012, as a request for a temporary restraining order, the purpose of which was to seek an immediate halt to the program, scheduled to begin on May 7, 2012.⁴²¹ The lawsuit was filed shortly after the ACLU had sent a letter to the Chief Administrator of the New Jersey MVC on late April 2012 that raised many of its concerns about Tru-ID.⁴²² The ACLU letter noted that REAL ID had been rejected in 25 states, and sought a meeting to discuss New Jersey's

⁴¹⁸ State of New Jersey, Motor Vehicle Commission, "Media Release: Christie Administration Announces New 'Skip the Trip' Drivers License and ID Mail Renewal Service for New Jerseyans New Process to Aid Implementation of Federal REAL ID Standards."

⁴¹⁹ Ibid.

⁴²⁰ Ibid.

⁴²¹ ACLU-NJ, *ACLU-NJ, et Al. v. Raymond P. Martinez, Et al.* Civil Action No. ____, *Brief in Support of Order to Show Cause with Temporary Restraints*, May 3, 2012.

⁴²² Deborah Jacobs, Executive Director, "Letter from the ACLU-New Jersey to Raymond P. Martinez, Chief Administrator New Jersey Motor Vehicles Commission," April 23, 2012.

implementation plan for TRU-ID.⁴²³ It does not appear that the meeting took place, and the lawsuit was filed, which led New Jersey to delay the implementation of Tru-ID.⁴²⁴

In October 2012, the court order issued in accordance with the State of New Jersey's agreement not to pursue its defense of the litigation, agreed instead that it would pursue rulemaking if it wished to pursue the program. The ACLU held a press conference to speak out about the court decision and the delay in TRU-ID implementation. "I am thrilled to see implementation of the REAL ID Act toppled in New Jersey," said Deborah Jacobs, the former ACLU-NJ executive director who served as an individual plaintiff in the case. "I hope the state's attempts to implement the REAL ID Act are now over, and we can join the majority of the states in our nation that have rejected the federal law as overly invasive and expensive."⁴²⁵

3. Basis of the Lawsuit and New Jersey's Next Steps

The main thrust of the New Jersey ACLU's challenge to TRU-ID centered on the claim that it violated New Jersey's Administrative Procedures Act, which according to the ACLU, "dictates any new rule or regulation requires, at minimum, public notice and the chance for citizen review." The ACLU further alleged that New Jersey had released "minimal information" about TRU-ID before the planned implementation and "sought no input from the public, legislators or stakeholders."⁴²⁶

Whether other states pursue court action to halt the implementation of REAL ID remains to be seen, but it may be instructive to examine the basis of the lawsuit, New Jersey's response, and what is happening now in New Jersey after its decision to stop pursuing TRU-ID. To prepare for litigation against the state of New Jersey, the ACLU had filed a request for documents under New Jersey's Open Public Records Act (OPRA),

⁴²³ Jacobs, "Letter from the ACLU-New Jersey to Raymond P. Martinez, Chief Administrator New Jersey Motor Vehicles Commission."

⁴²⁴ State of New Jersey, Motor Vehicle Commission, "TRU-ID Requirements Delayed Due to ACLU Court Motion," *Noodls*, accessed January 12, 2014, <http://www.noodls.com/viewNoodl/14226686/state-of-new-jersey-motor-vehicle-commission/tru-id-requirements-delayed-due-to-aclu-court-motion>.

⁴²⁵ ACLU-NJ, "State Settles ACLU-NJ Lawsuit by Agreeing to Drop TRU-ID Program," October 5, 2012, <http://www.aclu-nj.org/news/2012/10/05/drop-tru-id-program>.

⁴²⁶ *Ibid.*

on April 9, 2012 that sought information regarding what regulations New Jersey had promulgated regarding TRU-ID. It is apparent that the ACLU was seeking to establish that New Jersey had not promulgated any regulations. The State of New Jersey replied to the document request, noting, “TRU-ID is the program under which the State of New Jersey will implement the federal REAL ID Act and the accompanying regulations.”⁴²⁷ It further provided the ACLU with existing regulations promulgated by the MVC under the New Jersey Administrative Code “concerning identity requirements for obtaining a driver license or ID, which permits the MVC to make changes to the list of acceptable identity documents.”⁴²⁸ Thus, New Jersey’s position was essentially that no new rulemaking was required as it already had existing authority to make the changes it was making to the eligibility for and issuance process relating to New Jersey state identification documents.

It appears that New Jersey had a plausible legal argument against the ACLU challenge. It is not apparent why it did not more aggressively defend against the lawsuit, or what effect its abandonment of the lawsuit will have on its ability to be found to be in full compliance with REAL ID. Furthermore, it is not clear if the lawsuit reflects a new tactic on behalf of REAL ID opponents, of pursuing litigation under unique state level requirements, or to what extent those efforts would succeed. Instead of defending TRU-ID, New Jersey pursued its efforts under its existing 6-Point ID System. Notwithstanding the litigation, New Jersey has been particularly proactive in efforts to address fraud associated with state ID documents and has taken a variety of other measures that appear to have given the state and DHS some confidence that New Jersey is materially compliant with REAL ID.

4. New Jersey’s 6 Point ID System

Due to the settlement of the litigation, New Jersey continues to maintain its 6 Point ID licensing system. New Jersey’s website provides links to a brochure and a link a tool where persons seeking licenses and identification cards will be guided through the

⁴²⁷ Joseph F. Bruno, MVC Custodian of Records, Office of Legal and Regulatory Affairs, *New Jersey Response to ACLU Open Public Records Act Request*, April 24, 2012.

⁴²⁸ *Ibid.*

system, to demonstrate their eligibility for the license. As can be seen from the logo, and the accompanying explanation of the 6 Point ID System, New Jersey still stresses the security aspects of the program, and the website notes that the 6 Point ID verification system was designed to prevent identity theft (see Figure 13)⁴²⁹



The logo for the 6 Point ID Verification Program is a rounded rectangle divided into two main sections. The left section is yellow and contains a large red number '6' with the word 'point' in red lowercase letters below it. The right section is blue and contains the letters 'ID' in large white bold font, with 'Verification Program' in blue text below it. At the bottom of the logo, the slogan 'It's about protecting us all' is written in a black serif font.

6 Point ID verification

In order to obtain licenses and permits at MVC, you must prove your identity by passing 6 Point ID Verification. Select the documents you will use with one of the following tools:

- [Online Document Selector](#)
- [6 Point ID Brochure \[103k pdf\]](#)

En Español

- [Selector de documento verificación de 6 puntos](#)
- [Folleto para el Programa de Verificación de Identificaciones \[90k pdf\]](#)

6 Point ID Verification was designed to help prevent identity theft by ensuring that licenses are only issued with proper legal documents and verification. This requires you to prepare information prior to visiting an MVC Agency, possibly resulting in special document requests from other state agencies.

Figure 13. New Jersey's 6 Point ID System

A review of what that entails is useful to compare it to REAL ID requirements. According to the State of New Jersey's Motor Vehicle Commission, to obtain licenses and permits, individuals are required to prove their identity.⁴³⁰ New Jersey established the 6 Point ID Verification System to help prevent identity theft by requiring that licenses only be issued upon presentation of proper legal requirements and verification of the documents.⁴³¹ Individuals are advised that they must prepare information prior to visiting

⁴²⁹ State of New Jersey, Motor Vehicle Commission, "6 Point ID Verification," accessed February 8, 2014, <http://www.state.nj.us/mvc/Licenses/6PointID.htm>.

⁴³⁰ Ibid.

⁴³¹ Ibid.

the MVC, and that it may require special document requests from other state agencies.⁴³² Individuals demonstrate eligibility for a NJ license or identity document by presenting documents that demonstrate their eligibility to be licensed in New Jersey. New Jersey's licensing requirements consists of three elements. Individuals must present proof of residence, and they must present, pursuant to New Jersey state law, a SSN, which New Jersey advises will be checked against the records of the SSA.⁴³³ The third requirement relates to the need to establish an identity.

Residents must accumulate a total of six points, which is accomplished by presenting a combination of primary and secondary documents to demonstrate their identity by selecting a combination of documents specified by the MVC with individuals being required to provide at least one primary document and one secondary document. The primary documents include some for U.S. citizens and some for non-citizens, but secondary documents do not distinguish between U.S. citizens and non-citizens. Each category of document has a point scale, and individuals must accumulate six points to be eligible for a New Jersey license or identification document.

5. New Jersey's Anti-Fraud Efforts

Despite New Jersey's setbacks with the litigation, it nonetheless is one of the states closest to compliance based on the affirmative actions it has taken to improve the security of its driver's license system. Actions commenced even prior to the passage of the REAL ID Act. The non-profit group CSDL recognized New Jersey's efforts for a Secure Driver's License in October 2011, which awarded its National Security Excellence Award. The award was given for New Jersey's efforts in the furtherance of secure driver's license credentialing: 1) the security and integrity of the new enhanced digital driver license (EDDL), 2) the introduction of fraud prevention measures, and 3) the implementation of an effective identity verification process.⁴³⁴

⁴³² Ibid.

⁴³³ State of New Jersey, "New Jersey 6 Point ID Brochure," June 14, 2013, http://www.state.nj.us/mvc/pdf/Licenses/ident_ver_posterpint.pdf."

⁴³⁴ State of New Jersey, Motor Vehicle Commission, "MVC Honored with National Security Excellence Award," October 5, 2011, <http://www.state.nj.us/mvc/PressReleases/archives/2011/100511.htm>.

Upon receiving the award, the New Jersey's Director of the Office of Homeland Security affirmed New Jersey's commitment to secure identity documents by stating:

Receiving this award affirms the correctness of the state's strategy to adopt a secure driver license [that] guards against fraud. The Enhanced Digital Driver License prevents criminals from furthering their illegal activities through identity theft, which helps keep us safer.⁴³⁵

The press release that announced New Jersey's recognition by CSDL noted that the EDDL had been implemented in all 39 of New Jersey's driver's license offices as of May 2011, and built on New Jersey's efforts starting with the release of its first digital driver's license in 2004.⁴³⁶ According to the press release, the EDDL "is also considered materially compliant under REAL ID standards."⁴³⁷

In the area of secure identity documents, New Jersey has gone above and beyond measures taken by other states, and the MVC website notes that it has been recognized as having "one of the top two most thorough and secure ID verification policies in the country."⁴³⁸ New Jersey has established itself as a leader in the effort to take a full range of security measures as demonstrated through the examples of the EDDL and the adoption of facial recognition technology.

6. The Enhanced Digital Driver's License

The EDDL, while similar in appearance to the old license, "features more than 25 covert, overt and forensic features designed to reduce the fraud and abuse through updated technology and enhanced security features that are known only to the MVC and its law enforcement partners."⁴³⁹ New Jersey unveiled the EDDL on May 11, 2011 and

⁴³⁵ State of New Jersey, Motor Vehicle Commission, "MVC Honored with National Security Excellence Award."

⁴³⁶ Ibid.

⁴³⁷ Ibid.

⁴³⁸ State of New Jersey, Motor Vehicle Commission, "What Is the MVC?," accessed February 23, 2014, <http://www.state.nj.us/mvc/About/AboutMVC.htm>.

⁴³⁹ State of New Jersey, Motor Vehicle Commission, "MVC Honored with National Security Excellence Award."

noted that the enhanced driver's license was necessary because, as stated in the MVC press release:

The driver license is no longer a simple card that proves you are legally entitled to operate a motor vehicle, it is now the primary source of identification for most Americans and a source (breeder) document used for so many other pieces of identification.⁴⁴⁰

The importance of the EDDL to New Jersey's anti-fraud and crime-fighting efforts was highlighted by the appearance of the New Jersey Attorney General, Paula T. Dow, at the press conference who emphasized the importance of the EDDL to law enforcement efforts stating:

I want to commend the New Jersey Motor Vehicle Commission for its hard work in the creation of this new Enhanced Digital Driver License, as well as the multitude of law enforcement agencies that will assist in the investigation of those who seek to fraudulently obtain this new license, This cutting edge form of identification is one more tool available to all levels of law enforcement to stay one step ahead of criminals.⁴⁴¹

The MVC press release indicated that the software MVC was going to use for the EDDL would allow the MVC to take clear and accurate photos of each driver's license applicant.⁴⁴²

7. New Jersey's Use of Facial Recognition Technology

At the time of the award, the EDDL project team was involved in the early stages of implementing facial recognition technology to review over 16 million photo records. It would enable New Jersey, which in the coming year, was to implement central issuance of driver's licenses, to check for fraud, and catch that fraud before the licenses were issued to the applicant. Since that time, New Jersey has begun to see significant benefits from its use of facial recognition technology, which it refers to as *Operation Facial Scrub*

⁴⁴⁰ State of New Jersey, Motor Vehicle Commission, "NJ Motor Vehicle Chief, Attorney General and Homeland Security Director Unveil the State's New, More Secure Driver License," May 11, 2011, <http://www.state.nj.us/mvc/PressReleases/archives/2011/051111.htm>.

⁴⁴¹ Ibid.

⁴⁴² State of New Jersey, Motor Vehicle Commission, "MVC Honored with National Security Excellence Award."

that uses the technology to identify people seeking to obtain New Jersey driver's licenses using fraudulent identities.⁴⁴³ Since its inception, New Jersey's Attorney General's Office has filed 107 cases, with 69 filed during the last year. The announcement noted that the program has allowed it to "scrub" the nearly 23 million images for duplicates and through that process, New Jersey has identified 1.8 million records for further scrutiny, <http://www.washingtontimes.com/news/2014/mar/16/rules-that-keep-feds-from-trolling-facebook-twitte/?page=1> which ultimately resulted in 5,000 suspension cases being identified that required re-verification. It has also led to 2,100 cases identified for administrative suspensions, and 985 cases were referred for possible criminal charges, which has led to a partnership between the Attorney General's office and the county prosecutors.⁴⁴⁴ In addition to its efforts to address fraud within its state, New Jersey also shares information on fraud cases "via a secure website with the FBI's Joint Terrorism Task Force," as well as 23 state and federal partners and benefit providers, to include the DOS passport security, the SSA, and New Jersey's Departments of Labor and Human services to allow those entities to pursue cases involving fraud.⁴⁴⁵

8. New Jersey's Anti-Fraud Prosecutions

New Jersey officials have highlighted the problem of crime associated with identity theft by using two major operations as examples of the problem of crime associated with false identification documents. The largest prosecutions have been Operation Southern Drawn and Operation White Cloud, which, according to the MVC, have shown the direct relationship between fraudulent identification documents and the sale of stolen cars, car hijackings, and the sale of illegal drugs and guns.⁴⁴⁶

⁴⁴³ State of New Jersey, "Press Release: Attorney General & MVC Chief Announce New Charges Resulting From High-Tech Program 'Operational Facial Scrub' to Detect False Driver's Licenses," February 20, 2014, <http://www.state.nj.us/mvc/PressReleases/archives/2014/022014a.htm>.

⁴⁴⁴ State of New Jersey, "Press Release: Attorney General & MVC Chief Announce New Charges Resulting From High-Tech Program 'Operational Facial Scrub' to Detect False Driver's Licenses."

⁴⁴⁵ Ibid.

⁴⁴⁶ State of New Jersey, Motor Vehicle Commission, "MVC Honored with National Security Excellence Award."

On April 14, 2011, the New Jersey State Police issued a media release associated with these two large scale operations that resulted in the arrest of 13 people for crimes including the illegal sale of guns, drugs, and fraudulent IDs, and for auto theft by carjacking.⁴⁴⁷ In addition to the sale of fraudulent IDs, the illegal sale of drugs and 17 guns were facilitated by the use of the fraudulent identification documents. The media release included the following statements made by Peter T. Edge, special agent in charge of U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) in Newark, and MVC Chief Administrator Raymond P. Martinez, highlighting the role of fraudulent identity documents in facilitating criminal activity.

Document fraud and weapons trafficking is an extremely lucrative crime that can be challenging to investigate, but HSI agents, working with state and local law enforcement officials are determined to bring these criminals to justice. Fraudulent documents may be used to gain employment in critical infrastructure industries, obtain financial benefits and entitlements that are intended for U.S. citizens, and is a severe threat to our national security.

The MVC has zero tolerance for document fraud, abuse and identity theft and we remain vigilant in our effort to further protect the licensing process," said. "Today we stand tall with our law enforcement partners with the knowledge that when we work together, we will protect the integrity of our licensing system and the personal information of New Jerseyans."⁴⁴⁸

This investigation, which began in August 2010, uncovered a group of people making money through several different criminal enterprises. The investigation showed a relationship between the sales of fraudulent identification documents, the sale of stolen cars, carjackings, and the purchase of firearms from North Carolina.⁴⁴⁹

⁴⁴⁷ New Jersey State Police, *2011 News Release: 17 Guns Seized, 13 Arrested in Co-Op Cases Involving Gun Running, Carjacking, Drug Dealing, and Supplying Fraudulent IDs*, April 14, 2011, <http://www.njsp.org/news/pr041411.html>.

⁴⁴⁸ Ibid.

⁴⁴⁹ Ibid.

9. New Jersey's Media Coverage

New Jersey's newspaper editorials have diverged with each other on the issue of REAL ID with some favoring state implementation of REAL ID compliant standards and others opposing them. In addition, some editorial boards have themselves changed position on REAL ID. For example, shortly before the passage of REAL ID in 2005, several editorial boards took issue with the fact that REAL ID was about to be enacted on the basis of crafty maneuvering on the part of its sponsors, thereby passing an extensive mandate on states, and overriding efforts within and among states and the federal government to collaborate on setting standards to issue more secure licenses. The editorial boards of the Bergen County Record, and the *Newark Star-Ledger* generally took this approach.⁴⁵⁰ Two years later, the *Star-Ledger* went further, and in two editorials two months apart, called for New Jersey to join other states in a revolt against REAL ID, and for Congress to repeal the law.⁴⁵¹

However, several years later, the New Jersey newspapers diverged. On April 3, 2012, an editorial in the *Record* from Bergen County, New Jersey noted with approval, New Jersey's effort to launch the TRU-ID, New Jersey's version of REAL ID.⁴⁵² The editorial, while cautioning that the state needed to avoid implementation glitches that had led in the past to long lines, expressed its disagreement with the actions of 13 states that had passed laws prohibiting compliance with REAL ID. It explained its position noting:

We disagree. A more uniform driver's license system is necessary. Allowing each state to use its own formula makes it easy for would-be terrorists to head to the place with the laxest rules to get or renew a license. Putting a driver's license on par with a passport makes sense.⁴⁵³

In an editorial dated May 14, 2012, the *Newark Star-Ledger* urged that New Jersey withdraw from efforts to implement TRU-ID by citing its implementation costs

⁴⁵⁰ The Record, "A License for Trouble and a Boon for Identity Theft," May 6, 2005, LexisNexis Academic; see also, The Star-Ledger, "The Party of Centralized Power" July 19, 2005, LexisNexis Academic.

⁴⁵¹ The Star-Ledger, "Revoke Driver's License Law," March 4, 2007, LexisNexis Academic.

⁴⁵² The Record, "A Better License," April 3, 2012, LexisNexis Academic.

⁴⁵³ Ibid.

and what it termed its ultimate cost to privacy and security.⁴⁵⁴ As previously discussed, New Jersey did just that, and has returned to its 6 Point Verification system. This issue has not been covered in the media since that time—even following DHS’ announcement in December 2013 regarding phased enforcement.

C. MAINE

The State of Maine has been an outspoken opponent of REAL ID, while at the same time, demonstrating the clear vulnerabilities that exist in the state licensing systems that led to REAL ID’s passage and that have persuaded even opponents to address weaknesses in their state licensing systems. Maine was one of the states that actively resisted implementation of the law by initially passing a non-binding resolution asking Congress to repeal it, and asserting the Maine Legislature’s refusal to implement the law.⁴⁵⁵ It then passed an outright prohibition on implementing REAL ID. Maine law continues to prohibit state officials from complying with REAL ID requirements. However, the vulnerabilities of its licensing system, coupled with some degree of public pressure, have caused Maine to take what might be seen as a schizophrenic approach toward the issuance procedures for state driver’s license and identity documents. It also appears that Maine’s shifts are largely attributable to interesting, and shifting electoral politics in the state, including some infighting within the Democratic Party in Maine, and public pressure, that appear to have heavily influenced the state’s approach to REAL ID. The following discussion sets forth Maine’s REAL ID journey.

1. Maine’s Shifting Approach on Document Security

In January 2007, the Maine Legislature passed a nearly unanimous non-binding resolution urging Maine to reject REAL ID that alleged that it would be costly and difficult to implement, with costs estimated to reach \$185 million during the first five

⁴⁵⁴ The Star Ledger, “Revoke This License Plan New Jersey Should Back Out of Federal ID Program,” May 14, 2012, LexisNexis Academic.

⁴⁵⁵ Glenn Adams and The Associated Press, “Maine Says No Thanks to ID Act; U.S. Law Cumbersome, Costly Says Lawmakers,” *The Bangor Daily News*, accessed December 30, 2013, <http://archive.bangordailynews.com/2007/01/26/maine-says-no-thanks-to-id-act-u-s-law-cumbersome-costly-says-lawmakers/>.

years, and predicting that it would invite identity theft.⁴⁵⁶ The Senate Majority Leader, a Democrat, and sponsor of the resolution, expressed her view that REAL ID “will do nothing to make us safer, but it is our job as state legislators to protect the people of Maine from just this sort of dangerous federal mandate.”⁴⁵⁷ The Secretary of State, Matthew Dunlap, whose office administers state driver’s licenses in Maine through the Bureau of Motor Vehicles (BMV), issued a statement supporting the state legislature that cited an imbalance between security and privacy caused by REAL ID.

Maine lawmakers have delivered a clear signal to the Congress that the implications of Real ID are unacceptable. Lawmakers in Maine understand that security is a critical priority, but so is privacy, and most importantly, a security system should actually provide security. It is not at all clear that after all the expense and tribulation for citizens that Real ID would present that we would really be no safer.⁴⁵⁸

The statement also criticized REAL ID in comparison to the previous efforts of Maine Senator Susan Collins to implement document security efforts through the 2004 IRTPA, which has been previously discussed. In contrast to REAL ID, the 2004 law had a stakeholder process that “was designed to be implemented by the states in an absorbable way” but was replaced by Real ID.⁴⁵⁹

At the same time it was passing the non-binding resolution, the Maine legislature was introducing a companion piece of legislation that directed the Secretary of State to refuse to implement REAL ID.⁴⁶⁰ Enacted into law in 2007, it reads as follows:

§1411. Prohibition against participation in the federal REAL ID Act of 2005

⁴⁵⁶ Ibid.

⁴⁵⁷ Ibid.

⁴⁵⁸ State of Maine, “Maine Rejects Real ID Act: Joint Resolution Refutes Plan for National Identification Cards,” January 25, 2007, <http://www.maine.gov/sos/news/2007/RealIDAct.html>. (Although the statement is a bit unclear in its syntax, the Secretary of State was clearly expressing his disagreement with REAL ID).

⁴⁵⁹ Ibid.

⁴⁶⁰ Adams and Press, “Maine Says No Thanks to ID Act; U.S. Law Cumbersome, Costly Says Lawmakers.”

The State may not participate in the federal REAL ID Act of 2005, enacted as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Public Law 109–13. The Secretary of State may not amend the procedures for applying for a driver’s license or nondriver identification card under this chapter in a manner designed to conform to the federal REAL ID Act of 2005.

Maine is among a core group of states that have passed similar legislation to prohibit its state officials from taking action in furtherance of REAL ID.

2. The Political Backdrop Behind Maine’s Positions on REAL ID

An interesting dynamic in Maine has been the influence of the state’s electoral politics on its approach to REAL ID. Maine’s political party’s strength shows periods of stability, but recent electoral swings in Maine, which have shifted control of key political offices, alternating between the Republicans and the Democrats, have had an effect on legislative and policy approaches to REAL ID. The legislature was controlled by Republicans following the 2010 elections, and returned to Democratic Party control following the 2012 elections. Prior to 2010, Democrats controlled all the major state offices in Maine.⁴⁶¹ However, even when controlled by Democrats, the changes resulting from the political and policy shifts have been dramatic, and even some shifts occurring when only one party was in control, have no doubt proven confusing for state licensing officials, as well as the citizens of Maine.

3. Once Again--Leadership Matters: Secretary of State Matthew Dunlap

In Maine, the Secretary of State is responsible for administering the licensing of drivers, and is elected by the legislature. The current Secretary of State, Matthew Dunlap, began a second non-consecutive term in January 2013. He first served as Secretary of State beginning in 2005, serving until 2009, when the control of the Maine legislature reverted back to Republican control for two years. Dunlap was the Secretary of State at

⁴⁶¹ *Wikipedia*, s.v. “Political Party Strength in Maine,” last modified August 19, 2013, http://en.wikipedia.org/wiki/Political_party_strength_in_Maine; see also Maine.gov website, which contains election results information by year and office but does not show political party shifts <http://www.maine.gov/sos/cec/elec/prior1st.htm>.

the time of the non-binding resolution in 2007. The official website indicates that he has been actively involved in discussions surrounding identity security issues and makes clear that he favors the approach taken in the IRTPA with its negotiated rulemaking approach. Secretary of State Dunlap has a vested and understandable interest in that process, as the website and a *Bangor Daily News* article note that he had been personally involved in those efforts as a representative.⁴⁶²

The Secretary of State position in Maine is political in the sense that the politically elected members of the state legislature elect the Secretary of State. While it is not unusual to have such positions be political, it appears that Dunlap has played a particularly active role on the REAL ID issue, and much of the opposition to REAL ID has occurred under his watch as the official responsible for driver licensing issues in Maine. Dunlap is a long-time political figure in Maine politics, having run for and been elected to the legislature for four terms beginning in 1996, and then being elected Secretary of State by the legislature beginning in 2005, and commencing a non-consecutive term in January 2013. It also appears that Dunlap aspires to higher political office, having run unsuccessfully in the 2012 primary for the Senate seat then occupied by Olympia Snowe.⁴⁶³

Dunlap has been an outspoken opponent of REAL ID, and the Secretary of State's official website makes frequent references to that opposition, including his receipt of the ACLU's highest award, given in recognition to his opposition to REAL ID.⁴⁶⁴ The website notes that the ACLU cited Dunlap's opposition as "truly a patriotic act," and quoted from Dunlap's statement at the time of the award that:

I am truly honored to receive this award. Maine's political and community leaders have recognized REAL ID for what it truly is- a poorly thought out policy that fails to achieve its' supposed primary goal of improving

⁴⁶² The Bangor Daily News, "Dunlap Named to Serve on Federal Committee," accessed March 8, 2014, <http://archive.bangordailynews.com/2005/04/14/dunlap-named-to-serve-on-federal-committee/>.

⁴⁶³ Pollways, "Democrat Dunlap Declares," accessed March 8, 2014, <http://pollways.bangordailynews.com/2011/11/02/national/democrat-dunlap-declares/>.

⁴⁶⁴ State of Maine, Department of the Secretary of State, "Maine Civil Liberties Union Award," January 11, 2008, <http://www.maine.gov/sos/news/2008/MaineCivil.html>.

national security, while at the same time creating enormous concerns about the privacy of all Americans.⁴⁶⁵

The website highlights Dunlap's role in opposing REAL ID, the role of the legislature in passing the non-binding resolution in 2007, and later passage of the law to prohibit the state from expending state monies to comply with REAL ID.⁴⁶⁶ The site also touts Dunlap's "prominence in the national debate" as a consultant role for *ABC News* on matters related to REAL ID, and points readers to his upcoming televised remarks on the ABC show, "World News Tonight."⁴⁶⁷ He appears clearly to be a politician who has higher political aspirations, and may have found an issue with REAL ID that has resonated in Maine, or at least contributed, to a conflicted approach for the state. However, circumstances in Maine have evolved, which demonstrate political shifts and a conflicted approach for the state on the issue of REAL ID.

4. Security Vulnerabilities Exposed—Leading to a Gradual Shift

Notwithstanding its open defiance of REAL ID, Maine was forced to address vulnerabilities in its licensing system in 2008 because of the discovery that individuals were exploiting vulnerabilities in the states' driver's license issuance system, as well as pressure resulting from media coverage of those vulnerabilities. The specific vulnerability that Maine sought to address stemmed from a 2006 investigation conducted by the BMV, in conjunction with federal officials, into the transport of possible illegal aliens from Poland into Maine, via New York for the purposes of procuring Maine driver's licenses and state identification documents.⁴⁶⁸ Maine convened a working group under the auspices of the Secretary of State's office, which prepared a report dated December 5, 2007, and presented it to the Secretary of State.⁴⁶⁹ The report discussed the problem of how non-residents individuals of Maine could easily obtain driver's licenses,

⁴⁶⁵ Ibid.

⁴⁶⁶ Ibid.

⁴⁶⁷ State of Maine, Department of the Secretary of State, "Maine Civil Liberties Union Award."

⁴⁶⁸ Maine Department of Secretary of State, *Report of the Working Group Convened by the Secretary of State to Examine Laws Governing Eligibility and Documentation Requirements for Driver's Licenses and Non-Driver Identification Cards*, December 5, 2007.

⁴⁶⁹ Ibid.

and made recommendations on how to address the problem, primarily thorough legislative changes.⁴⁷⁰

In early 2008, the *Bangor Daily News* published a series of editorials highlighting recent embarrassments whereby individuals had been encouraged to come to Maine to obtain state issued driver's licenses because Maine did not check to see whether applicants for driver's licenses actually lived in Maine. One editorial urged the passage of a state law designed to ensure that individuals seeking licenses were, in fact, residents of Maine and supported additional state measures consistent with REAL ID requirements.⁴⁷¹ A similar editorial, issued two months later, reiterated its support for changes in Maine licensing and detailed the exchanges between the Governor's office and DHS officials that resulted in Maine proposing to make changes to its licensing procedures in exchange for an extension for Maine to avoid consequences from attaching to its failure to conform to REAL ID.⁴⁷²

5. Maine Tightens Its Driver License Issuance Process

The recommendations in the report became the basis of the modifications to the state's eligibility requirements for driver's licenses and identity documents. One action taken by Maine was to pass Public Law Chapter 648 in 2008. That law required applicants for a Maine license to establish that they are lawfully in the United States.⁴⁷³ The law took effect in November 2008, and as explained by the Secretary of State, made Maine driver's licenses valid only for the period of time that the individual was lawfully in the United States, with the validity of the driver's license expiring on the same date as did the individual's eligibility to remain in the United States.⁴⁷⁴ The Secretary of State's office made public appearances and issued notices advising Maine citizens of the new

⁴⁷⁰ Ibid.

⁴⁷¹ The Bangor Daily News, "Driver's License Fix," accessed December 29, 2013, <http://archive.bangordailynews.com/2008/02/25/drivers-license-fix/>.

⁴⁷² The Bangor Daily News, "License Failures," accessed December 29, 2013, <http://archive.bangordailynews.com/2008/04/09/license-failures/>.

⁴⁷³ State of Maine, "Secretary Dunlap Details New Requirements for Issuing Driver Licenses and State ID Cards," November 14, 2008, <http://www.maine.gov/sos/news/2008/new-dl-requirements.htm>.

⁴⁷⁴ Ibid.

requirements, and urged them to satisfy the lawful presence requirement by obtaining a certified copy of their birth certificate noting that it was the most common and easiest way to a lawful presence requirement.⁴⁷⁵ It also advised the public that it was a separate requirement to the need under Maine law, to establish residence.⁴⁷⁶ These requirements under Maine law stemmed from concerns that persons not resident in Maine, generally illegal aliens, were exploiting Maine's lax requirements for the issuance of driver's licenses and identification cards.

Legislation Enacted by Maine in Furtherance of REAL ID Requirements and Rolling Back Provisions Enacted by Maine to Comply with REAL ID

The Maine legislature took the following key steps toward implementing key provisions of REAL ID through its passage in 2008 of legislation known as An Act to Enhance the Security of State credentials.

- It required that state credentials only be issued to individuals determined to be lawfully in the United States
- It required Maine to tie the expiration of the document to the period of authorized stay in the United States
- It directed Maine officials to take a variety of actions to ensure that duplication of state credentials did not occur. To that end, the legislation called for Maine to use technology, such as facial recognition and biometric technology (fingerprints), and directed the Maine officials to explore ways to maintain and keep basic records of the photographs taken at the time that people applied for a state driver's license or non-driver identification card.⁴⁷⁷

Maine's current BMV website states that to get a Maine license, individuals must prove the following.

- That they are residents of Maine
- That they are citizens or are lawfully in the United States

⁴⁷⁵ State of Maine, "Secretary of State Matt Dunlap Reminds Motorists of Requirements for Obtaining Driver Licenses and State ID Cards," May 7, 2009, <http://www.maine.gov/sos/news/2009/legal-presence-reminder.htm>.

⁴⁷⁶ Ibid.

⁴⁷⁷ State of Maine, "Secretary Dunlap Details New Requirements for Issuing Driver Licenses and State ID Cards."

- That they have a Social Security number if one is not already on file; and if ineligible for a Social Security number, present immigration documents to help the BMV establish the ineligibility
- That their name change, if any, was legal by presenting appropriate documentation⁴⁷⁸

Nevertheless, the changes Maine made to its laws were made only grudgingly, in recognition of the fact that strong views existed in Maine against REAL ID and support for the law's repeal. Therefore, the statutory amendments included a provision that stated that if REAL ID were repealed, the Maine laws should be restored to what they were prior to the passage of REAL ID.⁴⁷⁹

6. Emerging Divisions Among Maine Democrats

By June 2008, Maine's governor at the time, Democrat John Baldacci, found himself in the awkward position of defending Maine's application for, and receipt of REAL ID demonstration grant program funding in excess of \$1 million dollars.⁴⁸⁰ This action, seen as inconsistent with Maine's state law prohibiting compliance with REAL ID, caused Baldacci to defend the application for the funding noting that the program's description specifically noted that states did not have to be REAL ID compliant to access the funds.⁴⁸¹ His public statement reflected the state's ambivalence on the issue of REAL ID, the Governor noted:

This is not about being compliant with a national ID system; this is about strengthening Maine's driver's licensees. I am determined we are going to do it and comply with the existing laws on the books.⁴⁸²

Further reflecting the tensions within the state on this issue, as well its complicated electoral politics, it appears that Secretary of State Dunlap was not made aware of the

⁴⁷⁸ State of Maine, "Obtaining a Driver's License," accessed March 8, 2014, <http://www.maine.gov/sos/bmv/licenses/getlicense.html>.

⁴⁷⁹ Maine State Legislature, "An Act to Enhance the Security of State Credentials, Maine Revised Statutes Annotated," 2008, <http://www.mainelegislature.org>.

⁴⁸⁰ Mal Leary and Capitol News Service, "Maine Receives \$1M Real ID Grant," *The Bangor Daily News*, accessed February 24, 2014, <http://archive.bangordailynews.com/2008/06/24/maine-receives-1m-real-id-grant/>.

⁴⁸¹ Ibid.

⁴⁸² Ibid.

grant application, and that it was sought by the state's Public Safety Commissioner, at the governor's direction, and without Dunlap being consulted.⁴⁸³ Dunlap told the *Bangor Daily News* that the first he first heard of the grant application from the paper's inquiry, and only thereafter, was made aware of the grant when the governor's chief of staff sent an email attaching the DHS grant news release from DHS. The Public Safety Commissioner disagreed, however, that Dunlap was unaware.⁴⁸⁴ It would be fair to say, that close coordination did not occur on the REAL ID demonstration grant ^{between} the Governor's office and the Secretary of State whose office oversees driver's license issuance.

Adding to the controversy on the grant issue is the fact that the documentation submitted in support of the grant identified a possible use of the purchase of software commonly used for facial recognition purposes, which is often used to identify whether a photograph matches that used on license under another name. This potential use of the grant funding was troubling to the Maine ACLU's Executive Director, Shenna Bellows, who stated:

We are concerned that both the governor and Commissioner Jordan are going against the will of the public and the Legislature in moving apparently ... full steam ahead in implementing Real ID. "That's why we are supporting the people's veto of Maine's Real ID law. Governor Baldacci and Commissioner Jordan are willingly embracing biometric technology and the Real ID privacy nightmare."⁴⁸⁵

7. The Pendulum Swings Back: The Fight to Roll Back REAL ID Compliance Measures

Nevertheless, Maine began another period of swings in the other direction and momentum swing in the other direction toward the limitations on REAL ID compliance. Yet, this issue caused significant ambivalence. Among REAL ID related editorials from the *Bangor Daily News* was one urging against the passage of a state bill that would have rolled back some of the measures taken the previous year to tighten the license issuance

⁴⁸³ Ibid.

⁴⁸⁴ Ibid.

⁴⁸⁵ Leary and Capitol News Service, "Maine Receives \$1M Real ID Grant."

process in Maine. While the editorial still generally opposed the REAL ID law, it acknowledged that improvements were needed, and measures undertaken by Maine in furtherance of REAL ID should not be undone.⁴⁸⁶

In 2011, at a time when Republicans controlled both the governor's office and the legislature, Maine took actions to both strengthen document security and bring itself closer to compliance, while also pursuing legislation that did the opposite. In March 2011, Maine's Republican Secretary of State, rolled out newly designed driver's licenses and identity documents, which incorporated a variety of security features recommended by AAMVA including ghost portraits, security indicia, and barcodes to protect against counterfeiting and forgery photo substitution, and cannibalization of cards (see Figure 14).⁴⁸⁷



Figure 14. Sample of a Maine Driver's License⁴⁸⁸

Maine's BMV website currently emphasizes the enhanced security features of the new driver's license design and recognizes the multiple uses of driver's licenses, to include entry into secure facilities. It notes that Maine has taken advantage of "state-of-the art" technology to enhance the security of the driver's license to include the use of

⁴⁸⁶ The Bangor Daily News, "Revisit Real ID," accessed December 30, 2013, <http://bangordailynews.com/2009/04/30/opinion/revisit-real-id/>.

⁴⁸⁷ State of Maine, "Secretary of State Summers Reveals Newly Designed Driver's License and Identification Cards," March 22, 2011, <http://www.maine.gov/sos/news/2011/newdriverlicense.htm>.

⁴⁸⁸ State of Maine, "Obtaining a Driver's License."

digital images and signatures that will increase the security of the license and make it more trustworthy in daily use.⁴⁸⁹

A couple of months later, on May 25, 2011, Maine enacted a law introduced as “An Act to Protect the Privacy of Maine Residents under the Driver’s License Laws.”⁴⁹⁰ The law amended Maine laws to address the privacy of personal information relating to state identity documents. It also had the effect of repealing a number of the very provisions that had been enacted to further compliance with REAL ID. The summary accompanying the legislation describes the legislation as follows: “This bill is a partial repeal of current Maine law enacted to comply with the requirements of the federal REAL ID Act of 2005.”⁴⁹¹ The legislation summarized as follows implemented a variety of provisions, some of which are in direct conflict with REAL ID requirements.

- Repeals the requirement that the Secretary of State issue driver’s licenses and non-driver identification cards only to individuals who present documentary evidence of legal presence in the United States
- Exempts SSNs in the possession of the Secretary of State from the definition of “public records” under Maine’s freedom of access laws
- Provides that the Secretary of State may not disseminate SSNs to any entity without legislative authorization
- Restricts the distribution and retention of digital information used to produce a license
- Prohibits the Secretary of State from the use of biometric technology, such as retinal scans, facial recognition or fingerprint technology, but not including digital photographs in the production or storing of license information
- Repeals the requirement that the Secretary of State participate in the federal Systematic Alien Verification for Entitlements Program, the

⁴⁸⁹ Ibid.

⁴⁹⁰ Maine State Legislature, “An Act to Protect the Privacy of Maine Residents Under the Driver’s License Laws, Maine Revised Statutes Annotated,” 2011, http://www.mainelegislature.org/legis/bills/display_ps.asp?paper=HP0803&PID=1456&snum=125&sec0; Maine State Legislature, “Summary of LD 1068 (HP 803): An Act To Protect the Privacy of Maine Residents under the Driver’s License Laws,” accessed January 19, 2014, <http://www.mainelegislature.org/LawMakerWeb/summary.asp?LD=1068&SessionID=9>.

⁴⁹¹ Open States, “Bill Text-HP 803-Maine 125th Legislature (2011–2012),” accessed January 29, 2014, <http://openstates.org/me/bills/125/HP803/documents/MED00003463/>.

centralized database system used and maintained by the U.S. Citizenship and Immigration Services

- Repeals the requirement that the Secretary of State study the most cost-effective technology to prevent driver's license or non-driver identification card duplication
- Provides that cost savings as a result of this act must be allocated to the Highway and Bridge Capital program within the DOT
- Does not change the current requirement that an applicant for a Maine driver's license or non-driver identification card must provide proof of residency
- Repeals the requirement that a license or non-driver identification card of a noncitizen or legal permanent resident expires at the end of the licensee's authorized duration of stay in the United States⁴⁹²

As can be seen, a number of the provisions conflict with REAL ID requirements; in particular, those limiting the ability to verify lawful status, or tie the expiration of the licenses to the period of authorized stay, and the limitation on use the use of biometric technology for the production or storage of license information. The Maine legislature's actions in defiance of REAL ID were the beginning of a series of actions reflecting Maine's vacillation regarding REAL ID. The many groups that came together to oppose REAL⁴⁹³ID in Maine reflect the civil liberties and libertarian strains that oppose REAL ID and which encompass groups ranging from the Maine Civil Liberties Union (MCLU), to the Cato Institute.⁴⁹⁴ The MCLU stressed that REAL ID served as a "one stop shop" for identity thieves because the cards would have embedded addresses and could be read by scanners.⁴⁹⁵

Despite Maine's strident position in opposition to REAL ID, Maine has had to grapple with the exploitation of its lax licensing procedures by those who would take advantage of its vulnerabilities. Those vulnerabilities ultimately led the Secretary of State to convene a working group to make recommendations for legislative improvements to

⁴⁹² Ibid.

⁴⁹³ Leary and Capitol News Service, "Maine Receives \$1M Real ID Grant."

⁴⁹⁴ Adams and The Associated Press, "Maine Says No Thanks to ID Act; U.S. Law Cumbersome, Costly Says Lawmakers."

⁴⁹⁵ Ibid.

address these vulnerabilities. As a result, Maine has also passed other laws to strengthen its driver licensing procedures regarding eligibility for driver's licenses in Maine.

8. Maine's Privacy Related Concerns About REAL ID

It appears that a major concern in Maine, and voiced by Secretary of State Dunlap, relates to threats to privacy. Those concerns appear to be exaggerated, but they appear to be genuinely held concerns. Maine's website makes broad claims against REAL ID, including the statement of the MCLU, that REAL ID would be "a huge threat to individual liberties," and that threats from identity thieves would be exacerbated because "REAL ID Act links driver's licenses and state ID cards to a national database."⁴⁹⁶ The latter assertion has been repeatedly rejected by DHS in its rulemaking documents and its related PIAs. Nevertheless, Maine has taken additional actions to strengthen protections for the privacy and security of driver's license information. On May 25, 2011, the governor signed into law measures designed to protect the privacy of Maine residents under the driver's license laws.⁴⁹⁷ The principal law, known as "An Act To Protect the Privacy of Maine Residents under the Driver's License Laws," did the following.

- Treats digital images and digitized signatures used to produce a license as confidential information that may only be distributed for use by a law enforcement agency in executing its functions or as otherwise authorized under the provisions of 18 United States Code, Section 2721.
- Authorizes the Secretary of State to store, record, and retain digital images and digitized signatures only for producing a license.
- Prohibits the Secretary of State from using biometric technology, including, but not limited to, retinal scanning, facial recognition or fingerprint technology, to produce a license or non-driver identification card. This subsection does not apply to digital images.
- Prohibits the Secretary of State from disseminating information collected under subsection 6 to any entity without specific authorization from the Legislature and provides for civil penalties of up to \$500 per violation.⁴⁹⁸

⁴⁹⁶ State of Maine, "Maine Rejects Real ID Act: Joint Resolution Refutes Plan for National Identification Cards."

⁴⁹⁷ Maine State Legislature, "Summary of LD 1068 (HP 803): An Act To Protect the Privacy of Maine Residents under the Driver's License Laws."

⁴⁹⁸ Open States, "Bill Text-HP 803-Maine 125th Legislature (2011–2012)."

Maine's experience is representative of the tensions and splits within a core group of states, and the consequences of its electoral shifts demonstrate a particularly tricky challenge for DHS as it seeks to encourage states to implement the law fully. The shifting state position also presents uncertainty for residents of such states.

XII. ANALYSIS AND FINDINGS

This paper has undertaken a broad examination of REAL ID; the controversy and concerns surrounding the legislation; responses to those concerns by DHS and others; and the progress by states on implementation efforts. It has also gone deeper into the controversies surrounding the legislation and the state implementation efforts by undertaking case studies of three states that are arrayed along the continuum of implementation milestones. The case studies demonstrate how different states have addressed REAL ID requirements, and explore how some of the issues of concern, interest groups, State leaders, and local politics have affected state implementation efforts. This thesis has also examined how DHS has attempted to address state concerns, and examined measures it has taken to facilitate and encourage State compliance, and how it is now approaching enforcement of REAL ID as a means of bringing all states into compliance. The following is an analysis of various issues examined in this paper, with the objective of making findings regarding how issues have been addressed and how and why compliance has been achieved or has proven elusive. That analysis and those findings will, in turn, inform the recommendations for DHS which follow in the final chapter.

A. REAL ID IS A NECESSARY AND APPROPRIATE TOOL TO ADDRESS THE PROBLEM OF INSECURE IDENTITIES

This paper began by stating that it would address the question of whether REAL ID was an effective and necessary *solution* to the problem of insecure driver's licenses and identity documents. It is this author's view that given the potential threats to national, individual, and institutional security, REAL ID is a necessary tool to address the threats facilitated by insecure identity documents, and that properly implemented it can be an effective way to address the range of threats. Given the complexities of the interrelated problems of document fraud, false identities and identity theft that can be used to further criminal behavior and terrorism, a strong measure like REAL ID was necessary. However, calling REAL ID the *solution* is too heavy a burden for a legislative scheme to bear. This is particularly so when the true measure of success against insecure licenses,

and ID cards lies in full and consistent implementation of the law across the country. Without consistency in implementation, vulnerabilities remain due to the persistence of weak links in the issuance of state identity documents. The success of REAL ID as a partial solution depends on the collective actions of all 56 states and territories, the efforts of DHS officials, and the support of other federal agencies, members the Congress, and the various Governors and State legislatures. All of those entities have to work collectively toward the same objectives in order to effectively address the problems posted by insecure state identity documents. This does not mean, however, that they should not work to address the concerns that have been raised and work toward acceptable solutions, recognizing that there are deep seated, sincerely held, and legitimate concerns with the REAL ID requirements.

B. DHS HAS WORKED TO ADDRESS THE RANGE OF CONCERNS RAISED BY CRITICS REGARDING THE LEGISLATION AND ITS IMPLEMENTATION CHALLENGES, BUT MUST DO MORE

Another question posed was whether DHS has effectively addressed state concerns related to REAL ID's implementation, such as: concerns about establishing a national ID card; threats to the federal/state balance of power contemplated by the Tenth Amendment; perceived threats to privacy; and the implementation costs. It is apparent that the uncertainty and concern that remains about these aspects of REAL ID have proven to be the most significant drivers of state opposition. DHS efforts to address the concerns are a work in progress and it remains to be seen whether DHS will effectively respond to and mitigate those concerns. There are encouraging signs, however, and DHS seems to have taken some measures to respond to concerns while giving states needed flexibility and time. By any measure, the changes required by REAL ID were substantial and its impact on individuals and States has been great. DHS has sought to respond to those concerns through its rulemaking efforts. Those efforts were extensive, while at the same time being relatively efficient and timely for a rulemaking effort of its size and scope. The REAL ID rulemaking, in the opinion of this writer, has been comprehensive, and largely transparent in identifying and responding to a range of significant issues posed by the law. DHS published an NPRM on March 9, 2007, processed over 21,000

comments related to the proposed rule, and published the final Rule on January 29, 2008. The rulemaking was accompanied by extensive Privacy Impact Assessments, as well as a detailed Regulatory Evaluation document of nearly 200 pages, published on January 17, 2008. in conjunction with the final rule. The latter document presents the benefits and costs of the minimum-standards required for driver license and ID card issuance under REAL ID.

There are major issues and concerns that DHS has sought to address through rulemaking and through the resources and support it has provided. It has been a mixed outcome so far in terms of DHS' ability to successfully address the concerns. The complexity and importance of these issues to States indicate that while much has been done, more can and should be done while recognizing that some States will never be satisfied with DHS efforts.

C. REAL ID IS NOT A NATIONAL ID BUT CAUTION IS WARRANTED

First, on the issue of whether REAL ID establishes a national ID, DHS has made repeated efforts to reject the notion that it was seeking to establish a national ID, whether in the form of a card, or a system of interconnected system of registries. This thesis addressed this issue by examining the traditional definition of a national ID system, examining the opinions of experts regarding what constitutes a national ID and what does not. It also compared REAL ID requirements to actions taken in furtherance of national ID systems by other countries for the purpose of clarifying the distinctions between actual national ID systems and the REAL ID requirements. The public perception and, as importantly, the political debates surrounding this issue remain mixed, with some emerging consensus that REAL does not constitutes a national ID.

Nevertheless the idea that REAL ID imposes a national ID system persists largely in jurisdictions that by their history, and often their politics, oppose federal regulatory measures and prefer as little federal intrusion as possible into what they see as State functions—such as driver licensing requirements. This opposition is represented by the handful of hold-out states that have passed states laws prohibiting compliance with REAL ID, with Maine representing those states in the case studies. This thesis has

addressed how traditional national IDs differ from REAL ID compliant documents. It has also sought to identify measures that DHS could take to reject basic elements of a national ID system, while at the same time making State licensing and identification systems more secure and less prone to errors, which are legitimate concerns with large, government run systems containing personal information.

D. REAL ID DOES NOT VIOLATE TENTH AMENDMENT PRINCIPLES OR CONSTITUTE AN UNFUNDED MANDATE, BUT FUNDING IS A KEY ISSUE FOR THE STATES

Federal laws and regulatory activity is often opposed on the basis that that it violates the Tenth Amendment, or that the federal government impose requirements on the states that constitute an unfunded mandate. This claim often resonates, particularly when the federal requirements coincide with periods of increasing regulatory activity and when economic conditions are such that states have smaller budgets, increasing needs, and less federal support. This has been the case with REAL ID, and there have been many assertions that REAL ID imposes an unfunded mandate on the states. While this paper has discussed that claim and largely determined that the law is not an unfunded mandate, the answer to that question is probably less important than the public perception. As a result, the need to assist states through additional resources to achieve the mutually beneficial outcome associated with secure identity documents seems obvious. Yet, the ancillary benefits for states also warrant equal effort on behalf of states to achieve REAL ID's document security objectives.

E. PRIVACY AND SAFEGUARDING OF PRIVATE INFORMATION ARE IMPORTANT CONSIDERATIONS AND ARE BEING ADDRESSED

The issue of government requirements and activities that may intrude on individual privacy and risk the exposure or theft of personal information is a significant concern raised by opponents of REAL ID. It is also one that is growing in public awareness and concern. This is particularly so due to revelations of private sector and government security breaches and the growing awareness of government collection of private information such as those exposed by Edward Snowden concerning the intelligence collection activities of the NSA. The requirement in the REAL ID

regulations that information be made available to other states and that each state utilize technology to store personal information on the identity documents themselves, has raised concerns from those that see the risks of potentially insecure systems and the impact on personal privacy. DHS has sought to allay those concerns, such as the use of RFID technology, choosing instead to keep the more low-tech, and lower capacity barcode technology standard for storage of REAL ID related information on driver's licenses and identity cards. At the same time, DHS, recognizing that technologies change rapidly has also left open the possibility that it will revisit the issue of the technology standard to be used--including the use of encryption of the information. It had rejected encryption when issuing the final rules, in order to ensure the accessibility of the information to law enforcement and facilitate the exchange of information among the various states and territories.

DHS has also declined to impose federal limitations on the access to such information. Instead, it has suggested that states address additional privacy protections at the state level. Such efforts could address concerns such as third party use of the information required by REAL ID, and maintained by the states in their records or on the cards themselves. DHS has suggested that states use model legislation such as proposed by AAMVA, and has provided examples of states that have enacted legislation to provide more stringent protections of information privacy at the local level. DHS' approach addresses the concerns of individual states in a more tailored manner.

F. CONCLUSIONS

This paper has sought to demonstrate the complex policy, legal, and practical issues posed by REAL ID. It has had a long, often rocky, and still incomplete journey toward its ultimate goal of achieving full implementation. It is this author's view that the successful completion of that journey is important for fundamental security issues and issues of trust between governmental institutions and the people with whom they interact.

Today, there remains inconsistency among the states regarding their adherence to the requirements of REAL ID. DHS has found that 21 states and territories are in full compliance with REAL ID, with another 35 still having taken few steps toward

compliance, or being in open defiance of the requirements. While states have made progress, not having all states in compliance means that weaknesses remain in the security and reliability of state identification documents. The delayed implementation has prevented DHS from restricting the use of those documents for the identified federal official purposes (currently, commercial air travel, access to nuclear facilities and access to federal buildings), in order to avoid significant burdens and inconvenience on the citizens of states that have not come into full compliance. This, in turn, means that the nation is tolerating the continued issuance and use of documents that are insecure and do not accomplish the stated purpose of increasing the security and reliability of identity documents. In addition to the impact that this has on the use of such documents for federal official purposes, the insecurity of those document has consequences that extend to the acquisition of federal benefits, the filing of federal tax returns, and insecure documents facilitate criminal activity such as identity theft that affects both businesses and individuals in the form of substantial monetary losses and other ancillary consequences. While much has been accomplished, much remains to be done to bring the remaining jurisdictions into full compliance. DHS has taken a necessary step by announcing the beginning of a phased enforcement through graduated consequences.

XIII. RECOMMENDATIONS

The security and reliability of state identification documents is dependent upon having the states adopt secure document verification procedures. As DHS continues to pursue full state compliance, some lessons and recommendations can guide DHS as it seeks to achieve full compliance. They fall into three general areas and are briefly discussed as follows.

A. ENGAGE WITH THE GENERAL PUBLIC TO EDUCATE THEM ON THE IMPORTANCE OF DOCUMENT SECURITY EFFORTS

DHS has generally directed its efforts at developing partnerships with states and allowing the states to be the principal drivers of REAL ID compliance efforts. Those partnerships and the primacy of the states' role should continue. DHS should consider engaging the public more directly on the importance of document security efforts. Recent concerns with identity theft present an opportunity to not only educate the public to help individuals avoid the consequences of identity theft and similar crimes, but to also inform the public about why the reliability and security of state identification documents needs to be improved to protect individuals, entities, and the government itself. It can use the opportunity to target public service announcements and undertake other forms of engagement differentiated between states in compliance and those that are not.

B. PARTNER WITH STATES THAT ARE IN FULL COMPLIANCE WITH REAL ID AND/OR ARE STRIVING TO BE IN COMPLIANCE AND RECRUIT STATE LEADERS THAT SUPPORT REAL ID AS NATIONAL SPOKESPERSONS

To date, 21 states have been found by DHS to be in full compliance with REAL ID. While DHS determines whether states are in compliance, with the exception of early efforts by Secretary Chertoff to partner with individual state governors to publicize REAL ID efforts in those states, DHS has not given much publicity as states achieve compliance. Instead, it has remained relatively neutral, and has acted as the arbitrator of compliance efforts, and occasionally, issuing a quiet press release on compliance updates. DHS should take a more active and publicly visible role in marking the achievements of

states that have reached the compliance milestone. Rather than letting those states announce their own compliance milestones, DHS should appear alongside state officials, and entities like AAMVA, and CSDL, to mark those achievements and use the opportunity to explain why the achievement matters.

C. DHS SHOULD DISPEL MYTHS ASSOCIATED WITH REAL ID AND ACTIVELY RESPOND TO CRITICS

DHS should take a page from the State of Delaware, and affirmatively address criticisms of REAL ID, and seek to dispel myths that have colored public perceptions relating to compliance with REAL ID. Given the current atmosphere with concerns about government activities affecting citizens, DHS has an opportunity to engage in ways that dispel myths, provides information to the public, and hopefully, increases public trust in government officials and programs. It should also enlist state leaders like Jennifer Cohan who have proven to be effective and credible spokespersons for how their states successfully achieved compliance and what outcomes and benefits have been seen by compliant states. DHS officials could, for example, appear at think tank discussions, hold press conferences with state officials, publish editorials, and make public appearances in states where implementation efforts are underway, as well as in states where controversies over compliance continue to exist.

D. UNDERTAKE ANNUAL REPORTING ON STATE PROGRESS ON REAL ID AND OUTCOMES WITHIN INDIVIDUAL STATES

This thesis has discussed DHS' August 2012 Report on State Progress on REAL ID, which was required by Congress. The report provided an excellent overview of DHS efforts in furtherance of REAL ID, including high-level discussion of tools and funding made available to states. It also served as an update for Congress on where the various states stood relative to full or material compliance with REAL ID. As useful as this report was, it was only produced one time, in fulfillment of a congressional requirement to report on state progress. It is recommended that DHS voluntarily produce this report on an annual basis, release it publicly, through a press conference and press release, and post the report on its website. It should also consider preparing more detailed annexes that

could be published as part of the annual report addressing distinct aspects of REAL ID implementation, to include issues, such as each states' compliance status, grant applications sought and awarded to states, ancillary effects of REAL ID implementation, such as state reporting on attempts to procure state identification document through fraud, and updated information on the effects of DHS' phased enforcement efforts. The information itself would serve to inform the public, allow states to see how they compare to other jurisdictions relative to REAL ID compliance, and demonstrate to Congress how grants are being allocated. Additional items could probably be reported in the monthly report, but the idea is to have DHS inform the public, the states, and Congress through ongoing reporting on progress being made on REAL ID implementation.

E. USE ENFORCEMENT AS AN OPPORTUNITY TO PERSUADE AND BUILD ALLIANCES AND AVOID DEEPENING DIVISIONS, WHILE PREPARING FOR LITIGATION

In December 2013, DHS announced it was beginning its phased enforcement of REAL ID, and would begin rejecting driver's licenses and state identification documents from non-REAL ID compliant states, beginning in April 2014. While the initial consequences would be mild, they would gradually increase toward the restriction of most concern, access to commercial airline flights, with that consequence commencing no sooner than 2016. Undoubtedly, any instance of enforcement will result in a period of publicity related to such event. DHS should not avoid publicity but should again use it as an opportunity to educate the public again. It should also take it as an opportunity to work with the affected state to offer assistance, and federal funding to ease the state's compliance burden and achieve compliance.

Along with enforcement is likely to come additional litigation. Surprisingly, little litigation appears to have been instituted against REAL ID, yet when citizens of non-compliant states begin to be affected by DHS enforcement efforts, it is likely that individuals or states will file lawsuits to prevent the consequences to holders of non-compliant licenses. DHS is better off addressing each situation in a way that will avoid litigation while focusing efforts on assisting the state to come into compliance, but it is likely that at least one of these actions will begin to proceed through the courts. It is

important that DHS, and the Department of Justice, vigorously defend against that litigation, or DHS risks having the system of secure identification unravel.

F. COMMIT TO REAL ID, AND SHOW THAT COMMITMENT THROUGH ACTIVE ASSISTANCE AND FUNDING

DHS can show its commitment thorough its defense against litigation as discussed in the preceding section. In addition, it should show its commitment to resist efforts, such as those that occurred in 2009, to pursue alternative legislation to REAL ID, such as that represented by PASS ID that loosened many of the requirements of REAL ID, which was described by one commenter as “dumbing down” the REAL ID requirements. While it seems unlikely to occur this many years into REAL ID implementation efforts, to do so would inject additional confusion into the understanding of states as to the requirements while likely introducing documents that have much less rigorous issuance standards, and thus, jeopardizing security.

One powerful motivator DHS continues to possess to show its commitment to states and the situation of the states is to continue to award grants to states for efforts related to REAL ID compliance, and actively to seek additional funding from Congress for such efforts.

G. IMPLEMENTATION OF RECOMMENDATIONS

Achieving full implementation of REAL ID will, first and foremost, contribute to greater assurance in knowing the true identity of individuals acquiring and using state driver’s license and identification documents. In turn, it will help to strengthen national security efforts by helping to identify terrorists and individuals with criminal backgrounds who seek to embed themselves in the United States without having federal, or state and local governments, and individuals with whom they interact, learn their true identities. It will give greater assurance that those who seek to avail themselves of the activities currently identified as “federal official purpose” have legitimate aims in accessing those federal services. It will potentially help to control illegal migration and residency in states that adhere to REAL ID requirements, as one of those requirements is that the states verify the status of individuals in the United States to limit issuance of

REAL ID compliant documentation to those individuals authorized to remain in the United States. Therefore, individuals who are unlawfully residing in the United States would not be eligible for REAL ID compliant licenses, and at best, would be issued driver's licenses or identification cards that have only limited use, and are unable to be used for federal official purposes.

Various potential impacts and measures of success are possible, depending on the position and interests of those affected. Success should give greater assurance to government, business, and individuals that people with whom they interact are who they say they are, and in turn, should have an effect on reducing activities and crimes associated with hiding an individual's identity. These beneficial effects could range from a reduction in terrorism, reductions in crimes against government entities, and against individuals. It would help law enforcement identify individuals who have been evading detection and capture using fraudulent documents.

Success initially can be measured quite simply by DHS reports as to how many states have been determined to be in full compliance with the provisions of REAL ID. DHS issues the reports periodically, and should continue to issue them, but in a more public manner than is currently the case. The ultimate measure of success by this standard is having DHS determine that all 56 jurisdictions subject to REAL ID are in full compliance. In other less objective ways, success may be more difficult to measure. Part of the intended purposes of the law and its implementation is that it will serve as a deterrent to the use of fraudulent identities and documents, and thus to some extent, its effects are in the absence of certain events or occurrence of certain phenomenon. Success can, however, be measured in ways, such as detecting the trend over time in attempts to secure state driver's licenses and identification documents through the use of fraudulent documents, through statistics showing hits against items like the SSA's Death Master File, which would reveal attempts to present documents (birth certificates) belonging to already deceased individuals. It could also be measured by reductions in identity theft related crimes in states that achieved full compliance, as opposed to states that have not come into full compliance.

The risks associated with implementing the recommendations of the thesis are relatively few. One risk may perhaps be that if additional funding is needed to achieve full compliance, that in this partisan atmosphere, it will not be possible to achieve consensus for additional funding. As a result, in the course of discussing the need for additional funding, some members of Congress would seek to scale back the provisions of REAL ID, and perhaps even seeking to revive inadequate alternatives to REAL ID, such as the Pass ID legislation promoted by DHS early in the Obama administration. Such legislation would be inadequate to obtain the security and law enforcement, and individual identity security benefits that REAL ID seeks to bring about.

The payoffs would be that the federal government, in facilitating access to those activities deemed to be federal official purposes under the act, would have greater assurances that the documents presented reflect the actual identity of the individual presenting them, and that the document was legitimately obtained. It would mean greater security in the transactions of individuals with the government, with business institutions, and with each other. It could help deter and address identity and identity theft related crime. A measure of success representing the results and benefits of REAL ID implementation would be the effect of REAL ID on identity theft. This success could encompass the tracking of data and publication of reports by the federal government or other entities showing whether REAL ID has resulted in reductions in identity theft, and other identity related crime and fraud, in states that have come into full compliance with REAL ID.

The costs of implementing REAL ID have not been insubstantial, and are one of the reasons states are opposed to REAL ID. The DHS estimate in the Notice of Proposed Rulemaking was projected to be \$7.88 billion over 10 years, and the total undiscounted, 11-year cost of the final rule was estimated by DHS to be \$9.9 billion.⁴⁹⁹ However, while the costs are substantial, the potential savings and reduction in losses due to identity theft and related offenses are substantially higher. For example, it is estimated that in 2010, losses to individuals from identity theft reached \$37 billion.⁵⁰⁰ It is unclear to what extent

⁴⁹⁹ Department of Homeland Security, *Final Rule*.

⁵⁰⁰ U.S. Government Accountability Office, *Driver's License Security*.

implementing the recommendations proposed by this thesis will add to, or reduce those implementation costs. However, it seems logical that proceeding with efficient implementation now, across states, will avoid incurring even higher costs associated with delayed implementation, such as those arising from changing technology, and uncoordinated efforts.

How long it takes to achieve full implementation by the states depends on various factors. Probably the largest driver will be the willingness of DHS to begin enforcing a firm deadline for the states to come into full compliance. DHS has extended that deadline several times, and after the last extension, which expired in January 2013, DHS provided a temporary deferment to states not in compliance and announced that in the fall of 2013, it would roll out a schedule of phased enforcement.⁵⁰¹ That schedule was finally released in December 2013 with the initial enforcement measures, which limit access to DHS facilities, just beginning. It is hoped that DHS in signaling its intention to pursue enforcement, can persuade states that have been postponing complying with REAL ID, to do so. That tactic will work for some, but not all states that have not come into full compliance.

The other factor that will affect the implementation will be the availability of funding at the state level, as well as the availability of Congressional appropriations and DHS grants to assist states with defraying the costs of implementation. A goal of publishing this thesis is to drive the dialogue among, and between those within state and federal legislatures and those responsible for allocating federal grants, to make funding available to facilitate full implementation.

As noted, the ultimate measure of success is straightforward. It is when DHS determines that all states and territories subject to REAL ID requirements have come into full compliance with the federal standards for the issuance of state driver's license and identity documents. To date, only 21 jurisdictions have been found to be in full compliance with 35 others in various stages of compliance. Until then, the regular

⁵⁰¹ Department of Homeland Security, "DHS Determines 13 States Meet REAL ID Standards," accessed December 2, 2013, <http://www.dhs.gov/news/2012/12/20/dhs-determines-13-states-meet-real-id-standards>.

addition to the list of compliant jurisdictions, through regular and consistent reporting by DHS, perhaps on a quarterly basis of state found to be compliance, could be implemented. Another measure of interim success would be the roll out of phased consequences for states that remain non-compliant. While states are not required to come into compliance, no incentive exists for states to come into compliance if their citizens are in no better position in terms of access to the activities deemed federal official purposes, if consequences are not enforced for non-compliant states.

On a more fundamental level, it should be acknowledged that REAL ID represents an increasing trend and desire, particularly post-9/11, to address the “problem of identification” and satisfy the “persistent impulse to identify individuals with recourse to official records” largely because of a desire to “establish a relationship of trust between individuals and the institutions with which they interact in their daily lives.” As stated by one researcher who has studied REAL ID:

. . . the scale of modern society is such that institutions cannot possibly know each individual on a personal basis and thus they require some form of confirmation that establishes that individuals are who they claim to be. Individuals themselves must establish their consistent identity over time and across distance for their own well-being.⁵⁰²

REAL ID can be seen as promoting the security of society, and in addition, improving the well being of individuals through its efforts to improve the security and reliability of state identity documents. Looked at presently, REAL ID “outlines a desired policy outcome rather than actually existing administrative system.”⁵⁰³ Whether, and when that desired policy outcome becomes an existing, fully functioning system remains to be seen. However, after nearly nine years, the end of the REAL ID journey is within sight.

⁵⁰² Gates, “The United States REAL ID Act and the Securitization of Identity,” in *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, 220.

⁵⁰³ *Ibid.*, 226.

APPENDIX A. IDENTIFICATION DOCUMENTS HELD BY THE 9/11 HIJACKERS⁵⁰⁴

Identification Documents of the 9/11 Hijackers	
Mohamed Atta FL DL, 05/02/01	Marwan al Shehhi FL DL, 04/12/01 FL DL duplicate, 6/19/01
Khalid al Mihdhar CA DL, 04/05/00 USA ID card, 07/10/01 VA ID card, 08/01/01	Nawaf al Hazmi CA DL, 04/05/00 FL DL, 06/25/01 USA ID card, 07/10/01 VA ID card, 08/02/01
Hani Hanjour AZ DL, 11/29/91 FL ID card, 04/15/96 VA ID card, 08/01/01 Failed VA DL test, 08/02/01 MD ID card, 09/05/01	Ziad Jarrah FL DL, 05/02/01 FL DL duplicate 5/24/01 VA ID card, 08/29/01
Satam al Suqami No DL or ID card	Waleed al Shehri FL DL, 05/04/01 (duplicate issued with different address, 05/05/01)
Ahmed al Ghamdi USA ID card, 07/2001 VA ID card, 08/02/2001	Majed Moqed USA ID card, 07/2001 VA ID card, 08/02/2001
Hamza al Ghamdi FL ID card, 06/26/01 FL DL, 07/02/01 (duplicate issued 08/27/01)	Mohand al Shehri FL ID card, 07/02/01
Ahmed al Nami FL DL, 06/29/01	Wail al Shehri FL DL, 07/03/01
Ahmed al Haznawi FL DL, 07/10/00 (duplicate issued 09/07/01)	Fayez Banihammad FL ID, 07/10/01
Saeed al Ghamdi FL ID card, 07/10/01	Salem al Hazmi USA ID card, 07/01/01 ¹⁹⁷ VA ID card, 08/02/01
Abdul Aziz al Omari USA ID card, 07/10/2001 VA ID card, 08/02/2001	

⁵⁰⁴ National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, 44.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. EVVE IMPLEMENTATION AS OF JUNE 2012⁵⁰⁵

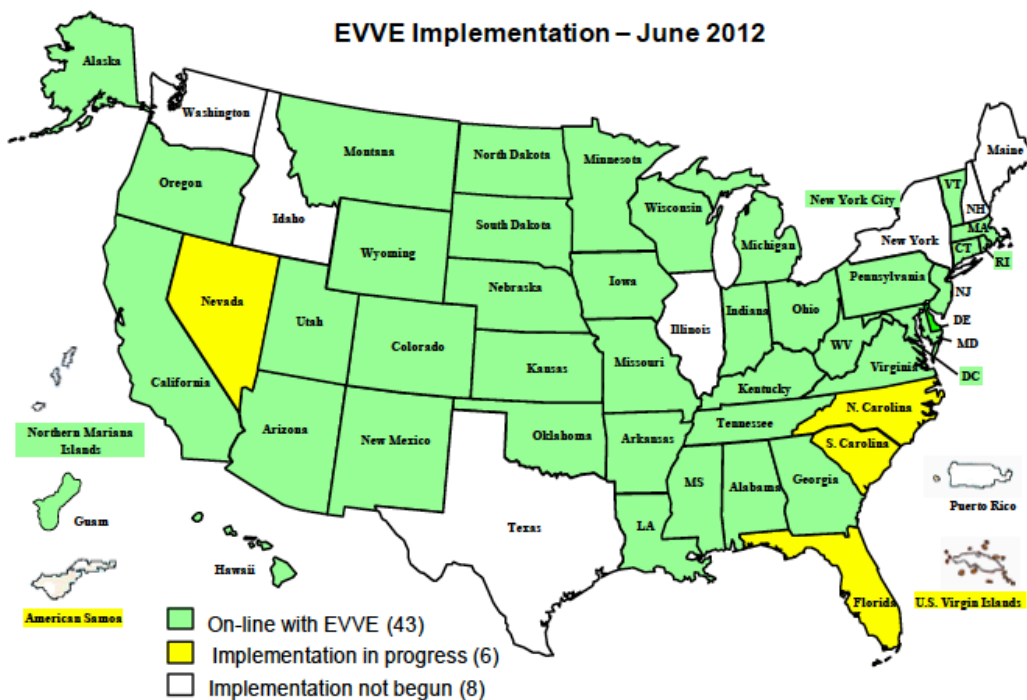
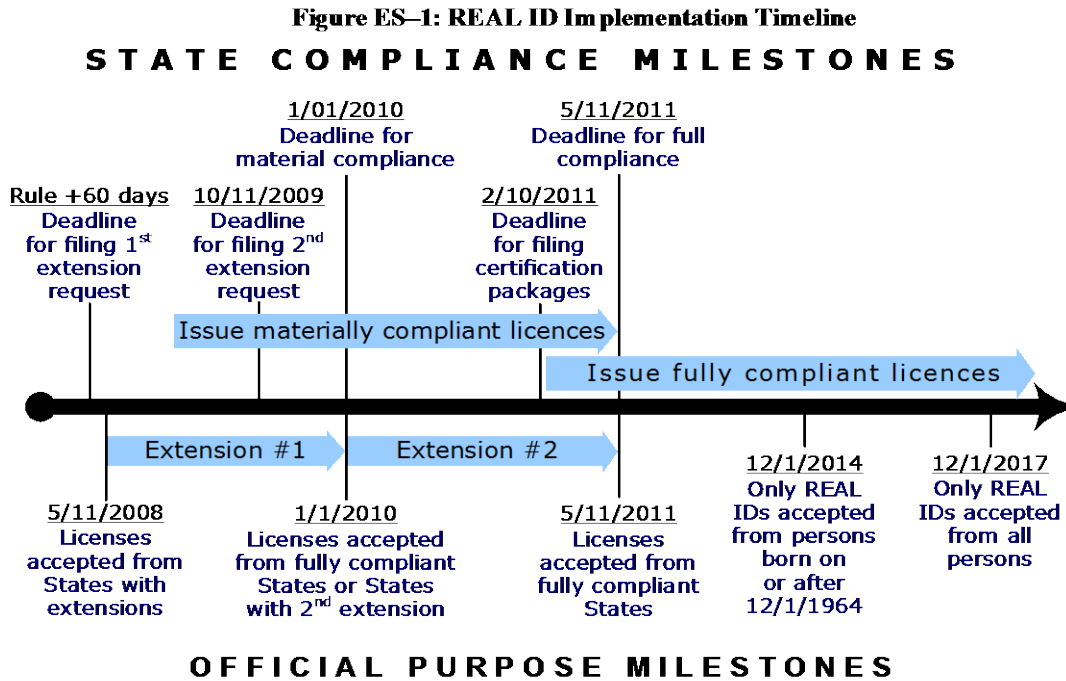


Figure 8. State Birth Records That Can Be Verified via EVVE

⁵⁰⁵ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 23.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. REAL ID IMPLEMENTATION TIMELINE AS PUBLISHED IN MARCH 2008 REGULATORY EVALUATION FINAL RULEMAKING⁵⁰⁶



⁵⁰⁶ Department of Homeland Security, *Regulatory Evaluation Final Rulemaking* 6 CFR Part 37.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. DHS' 18 MATERIAL COMPLIANCE BENCHMARKS DEPARTMENT OF HOMELAND SECURITY⁵⁰⁷

Does the State:	
1.	Subject each applicant to a mandatory facial image capture and retain such image even if a driver license (DL) or identification card (ID) is not issued
2.	Have each applicant sign a declaration under penalty of perjury that the information presented is true and correct, and retain this declaration.
3.	Require an individual to present at least one of the source documents listed in subsections 37.11 (c)(1)(i) through (x) when establishing identity
4.	Require documentation of: <ul style="list-style-type: none"> • Date of birth • Address of principal residence • Social Security Number • Evidence of lawful status
5.	Have a documented exceptions process.
6.	Make reasonable efforts to ensure that the applicant does not have more than one DL or ID already issued by that State under a different identity
7.	Verify lawful status through SAVE or another method approved by DHS
8.	Verify Social Security account numbers with the Social Security Administration
9.	Issue DL and IDs that contain Level 1, 2 and 3 integrated security features
10.	Surface of cards include the following printed information in Latin alpha-numeric characters: <ul style="list-style-type: none"> • Full legal name • Address of principal residence • Date of birth • Signature [with exceptions] • Gender • Date of transaction • Unique DL/ID number • Expiration date • Full facial digital photograph • State or territory of issuance
11.	Commit to mark materially compliant licenses with a DHS-approved security marking ‡ #
12.	Issue temporary or limited-term licenses to all individuals with temporary lawful status and tie license validity to the end of lawful status
13.	Have a documented security plan for DMV operations
14.	Have protections in place to ensure the security of personally identifiable information
15.	Require all employees handling source documents or issuing DLs or IDs to attend and complete fraudulent document recognition and security awareness training
16.	Conduct name-based and fingerprint-based criminal history and employment eligibility checks on all employees in covered positions or alternative procedure approved by DHS
17.	Commit to be in material compliance with the regulation no later than January 1, 2010.‡ #
18.	Clearly state on the face of non-compliant DLs or IDs that the card is not acceptable for official purposes ‡

‡ — States not required to report to FEMA on this benchmark.

— Benchmark superseded by indefinite stay of material compliance deadline.

Table 1. Synopsis of Material Compliance Benchmarks

⁵⁰⁷ Department of Homeland Security, *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, 5.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. THE EXTENDED TABLE OF CONTENTS FROM THE REGULATORY ASSESSMENT OF COSTS AND BENEFITS THAT ACCOMPANIED THE REAL ID FINAL RULE⁵⁰⁸

EXTENDED TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
OVERVIEW	1
ASSUMPTIONS	2
SUMMARY OF MAJOR DIFFERENCES BETWEEN THE FINAL RULE AND NPRM	6
COSTS AND BENEFITS	8
ECONOMIC COSTS	8
ESTIMATED BENEFITS	11
REGULATORY SUMMARY	12
EXECUTIVE ORDER 12866 ASSESSMENT	12
I. INTRODUCTION	14
II. A NOTE ON PUBLIC COMMENTS	15
III. STATUS QUO	15
III.A. USE OF IDENTITY DOCUMENTS	15
III.B. POPULATION	16
III.C. APPLICATIONS	18
III.C.1. <i>Pre-enrollment</i>	19
III.C.2. <i>Queuing</i>	19
III.C.3. <i>Customer Service</i>	20
III.C.4. <i>Acceptable source documents</i>	20
III.C.5. <i>Validity Periods</i>	22
III.C.6. <i>Remote reissuance and renewals</i>	23
III.C.7. <i>Front-end application processing</i>	24
III.D. VERIFICATION	25
III.D.1. <i>Identity, lawful status and SSN</i>	25
III.D.2. <i>Address of principal residence</i>	27
III.D.3. <i>Termination of license in other jurisdictions</i>	28
III.E. CARD PRODUCTION AND ISSUANCE	28
III.E.1. <i>Document Issuance</i>	29
III.E.2. <i>Design/Layout</i>	29
III.E.3. <i>Security Features</i>	30
III.E.4. <i>Card production costs</i>	30
III.E.5. <i>Machine Readable Technology</i>	32
III.F. DATA	32
III.F.1. <i>Imaging and storage</i>	32
III.F.2. <i>DMV Databases and connectivity</i>	33
III.G. SECURITY	33
III.G.1. <i>Physical security of facilities and materials</i>	34
III.G.2. <i>Employee background checks</i>	34
III.G.3. <i>Fraudulent document recognition training</i>	35
IV. DISCUSSION OF THE FINAL RULE	35
IV.A. USE OF IDENTITY DOCUMENTS	35
IV.B. POPULATION	36
IV.C. APPLICATIONS	37
IV.C.1. <i>Pre-enrollment</i>	37
IV.C.2. <i>Queuing</i>	37
IV.C.3. <i>Customer Service</i>	38
IV.C.4. <i>Acceptable Source Documents</i>	38
IV.C.5. <i>Validity period</i>	39
IV.C.6. <i>Remote renewals</i>	39

⁵⁰⁸ Department of Homeland Security, *Regulatory Evaluation Final Rulemaking 6 CFR Part 37*, iv–vi.

IV.C.7.	Front-end application processing	40
IV.D.	VERIFICATION	40
IV.D.1.	Identity, lawful status and SSN	40
IV.D.2.	Address of principal residence	42
IV.D.3.	Termination of license in other jurisdictions	42
IV.E.	CARD PRODUCTION AND ISSUANCE	42
IV.E.1.	Document issuance	43
IV.E.2.	Design/Layout	43
IV.E.3.	Security Features	43
IV.E.4.	Machine Readable Technology	44
IV.F.	DATA	44
IV.F.1.	Imaging and storage	44
IV.F.2.	DMV databases and connectivity	44
IV.G.	SECURITY	45
IV.G.1.	Physical security of facilities and materials	45
IV.G.2.	Employee background checks	45
IV.G.3.	Fraudulent document recognition training	45
IV.H.	CERTIFICATION AND COMPLIANCE	46
	COST ESTIMATES AND ALTERNATIVES ANALYSIS	46
V.A.	ASSUMPTIONS, UNCERTAINTY, AND BALANCING CONFLICTING PUBLIC NEEDS	50
V.A.1.	Assumptions: Final versus NPRM	50
V.A.2.	Estimate Uncertainty	56
V.B.	USE OF IDENTITY DOCUMENTS	65
V.C.	POPULATION	72
V.D.	APPLICATIONS	76
V.D.1.	Pre-enrollment	77
V.D.2.	Customer service	83
V.D.3.	Applicant visits	87
V.D.4.	Acceptable source documents	89
V.D.5.	Remote re-issuance	90
V.D.6.	Front-end application processing	90
V.E.	VERIFICATION	90
V.E.1.	Identity and lawful status documents	91
V.E.2.	Address of principal residence	96
V.E.3.	Social Security Number	97
V.F.	CARD PRODUCTION AND ISSUANCE	100
V.F.1.	Document issuance	101
V.F.2.	Design/Layout	104
V.F.3.	Security Features	105
V.F.4.	Card production costs	105
V.F.5.	Machine Readable Technology	110
V.G.	DATA	113
V.G.1.	State systems	114
V.G.2.	National Systems	118
V.G.3.	Manual Verifications	120
V.H.	SECURITY	121
V.H.1.	Physical security of facilities and materials	122
V.H.2.	Employee background checks	123
V.H.3.	Fraudulent document recognition training	124
V.I.	CERTIFICATION AND COMPLIANCE	127
V.I.1.	State certification	128
V.I.2.	Federal program office	128
I.	BENEFITS ANALYSIS	129
V.I.A.	OVERVIEW	129

VI.B.	LIMITATIONS:	131
VI.C.	REVIEW OF PUBLIC COMMENTS	131
VI.D.	PRIMARY BENEFIT OF REAL ID	132
VI.D.1.	<i>Break-Even Analysis</i>	132
VI.D.2.	<i>Other Direct Impacts to Be Considered</i>	142
VI.E.	ANCILLARY BENEFITS OF REAL ID: OVERVIEW	145
VI.E.1.	<i>Identity Theft</i>	145
VI.E.2.	<i>Unqualified Driving and Traffic Accidents</i>	146
VI.E.3.	<i>Other Ancillary Benefits of REAL ID</i>	148
VI.F.	ENABLED OPPORTUNITIES	149
VI.G.	CONCLUSION	149
VII.	FINAL REGULATORY FLEXIBILITY ANALYSIS	151
VIII.	INTERNATIONAL TRADE	155
IX.	UNFUNDED MANDATES ANALYSIS	156
	APPENDIX A: POPULATIONS	157
	APPENDIX B: ACQUIRING SOURCE DOCUMENTS	162
	APPENDIX C: CURRENT VERIFICATIONS	172
	APPENDIX D: HOURLY COST OF COMPENSATION	175
	APPENDIX E: DISCUSSION OF OPPORTUNITY COSTS	178
	APPENDIX F: MARGINAL TIME ESTIMATES FOR APPLICATIONS	192

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. NOTICE ON REAL-ID FUNDING AVAILABILITY MADE BY FEMA⁵⁰⁹

U.S. Department of Homeland Security
Washington, DC 20472



Grant Programs Directorate Information Bulletin
No. 277
January 28, 2008

TO: All State Administrative Agency Heads
All State Administrative Agency Points of Contact
All State Homeland Security Directors
All State Drivers' Licensing Authorities

FROM: W. Ross Ashley
Assistant Administrator
Grant Programs Directorate
Federal Emergency Management Agency

SUBJECT: Consolidation of Fiscal Year (FY) 2008 REAL ID Funding Availability

The purpose of this Information Bulletin (IB) is to provide All State Agency contacts with an updated notice of funding availability for FY 2008 REAL ID funding initiatives. On December 18th 2007, FEMA's Grant Programs Directorate (GPD) released grant guidance for \$31.3 million under the FY 2008 REAL ID Demonstration Grant Program. On December 26, 2007, the President signed the FY 2008 Omnibus Appropriations Bill (Public Law 110-5), which appropriates an additional \$50 million in REAL ID grants to States. In order to streamline the REAL ID grant process, FEMA/GPD plans to consolidate the \$50 million appropriation with the \$31.3 million recently announced. States will use the FY 2008 REAL ID Demonstration Grant Program solicitation to submit applications for REAL ID grant funding totaling \$79.875 million. The total amount available for grant funding reflects deductions legislatively authorized and taken by DHS for program management and administration of REAL ID grant funds. Demonstration grant program applications will now be due March 7, 2008. States that had not planned to submit grant applications before now may reconsider applying for this consolidated REAL ID funding opportunity. States are reminded to submit their REAL ID grant applications through www.grants.gov using the FY 2008 REAL ID Demonstration Grant Program guidance.

Eligible applicants for REAL ID funding are State Drivers' Licensing Authorities (DLA) which in most cases would be State Motor Vehicle Administrations (MVA) or State Department of Motor Vehicles (DMV). In some cases, other agencies such as State Departments of Public Safety would be eligible grant applicants if these agencies are responsible for DLA's in their State.

Should you have any questions, please contact your Preparedness Officer at (800) 368-6498.

www.fema.gov

⁵⁰⁹ Federal Emergency Management Administration, *Grant Programs Directorate Information Bulletin No. 277 January 28, 2008: Consolidation of Fiscal Year (FY) 2008 REAL ID Funding Availability.*

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. CENTER FOR IMMIGRATION STUDIES GRANT ALLOCATION BY JURISDICTION⁵¹⁰

Center for Immigration Studies

Driver License Security Implementation: System Connectivity and Grant Allocation by Jurisdiction				
Jurisdiction	REAL ID Benchmarks Met to Date -18 by May 11, 2011 -all enrolled by 2017 ¹	CDLIS ² & NDR Commercial DL and Nat'l Driver Registry (problem driver)	SSOLV ³ (SSN check)	SAVE ⁴ (lawful presence required) *ID expires at end of authorized stay
Alabama	18 + compliance mark	✓	✓	✓ ^A
Alaska	7	✓	✓	✓
American Samoa ¹⁰	9			
Arizona	12 (+1 partial)	✓	✓	✓ ^A
Arkansas	17	✓	✓	✓ ^A
California	11 (+3 partial)	✓	✓	✓ ^A
Colorado	18	✓	✓	✓ ^A
Connecticut	17	✓	✓	✓
Delaware	18 + compliance mark	✓	✓	✓ ^A
District of Columbia	14	✓	✓	✓ ^A
Florida	18 + compliance mark	✓	✓	✓ ^A
Georgia	15	✓	✓	✓ ^A
Guam	5			
Hawaii	3 (+2 partial)	✓	✓	✓ ¹¹
Idaho	13 (+3 partial)	✓	✓	✓ ^A
Illinois	9 (+9 partial)	✓	✓	✓
Indiana	18 + compliance mark	✓	✓	✓ ^A
Iowa	18	✓	✓	✓ ^A
Kansas	18 + compliance mark	✓	✓	✓
Kentucky	18	✓	✓	✓ ^A
Louisiana	9 (+4 partial)	✓	✓	✓ ^A
Maine	8 (+3 partial)	✓	✓	✓ ^A
Maryland	18	✓	✓	✓ ¹¹
Massachusetts	6 (+2 partial)	✓	✓	✓
Michigan	12	✓	✓ ¹¹	✓ ^A
Minnesota	11	✓	✓ ¹¹	✓ ^A
Mississippi	18	✓	✓	✓
Missouri	13 (+2 partial)	✓	✓	✓ ^A
Montana	9 ²⁰	✓	✓	✓ ^A
Nebraska	16 (+2 partial)	✓	✓	✓
Nevada	17	✓	✓	✓ ^A
New Hampshire	11 (+4 partial)	✓	✓	✓
New Jersey	9	✓	✓	✓ ^A
New Mexico	10 (+3 partial)	✓	✓	
New York	16	✓	✓	✓
North Carolina	12 (+2 partial)	✓	✓	✓ ^A
North Dakota	15	✓	✓	✓ ^A
Northern Mariana Islands	N/A			
Ohio	13	✓	✓	✓ ^A
Oklahoma	8 ²⁰	✓	✓ ¹¹	✓ ^A
Oregon	13	✓	✓	✓
Pennsylvania	13	✓	✓	✓ ^A
Puerto Rico	13			
Rhode Island	9	✓	✓	✓
South Carolina	13 (+1 partial)	✓	✓	✓ ^A
South Dakota	18 + compliance mark	✓	✓	✓ ^A
Tennessee	14	✓	✓	✓ ^A
Texas	10 (+3 partial)	✓	✓	✓ ^A
US Virgin Islands	4			
Utah	18 + compliance mark	✓	✓	✓ ¹¹
Vermont	9 (+5 partial)	✓	✓	✓ ^A
Virginia	5 (+10 partial)	✓	✓	✓ ^A
Washington	9 ²⁰	✓	✓	
West Virginia	14	✓	✓	✓ ^A
Wisconsin	14	✓	✓	✓ ^A
Wyoming	17	✓	✓	✓ ^A

⁵¹⁰ Kephart, “Real ID Implementation Less Expensive, Doable, and Helpful in Reducing Fraud.”

Center for Immigration Studies

EVVE ⁵ (digitized vital records) *DMV checks EVVE records	Grant Allocation FY08 (\$79.875 mil.) ⁶	Grant Allocation FY09 Part I (\$48.575 mil.) ⁷	Grant Allocation FY10 Part II (\$48.000 mil.)	Total Grant Allocation to Date (\$176.45 mil.) [total expenditure to comply with 18 benchmarks]
✓	\$500,000	\$1,060,774	\$1,098,276	\$2,209,050 [\$15,061,141] ⁸
	0 ⁹	\$600,000	N/A	\$600,000
	\$300,000	\$600,000	\$651,877	\$1,551,877
✓ (partial) ¹¹	\$2,721,110	\$1,060,774	\$1,098,276	\$4,880,160
✓	\$891,887	\$755,987	\$800,677	\$2,448,551
✓ ¹¹	\$3,200,000	\$1,648,250	\$1,656,999	\$6,505,249
✓ (partial) ¹¹	\$1,169,678	\$755,987	\$800,677	\$2,726,342
✓	\$1,901,846	\$755,987	\$800,677	\$3,458,510
	\$500,000	\$600,000	\$651,877	\$1,751,877 [\$3,075,000] ¹²
	\$500,000	\$600,000	\$651,877	\$1,751,877
	\$3,750,926 ¹³	\$1,648,250	\$1,656,999	\$7,056,175 [\$945,030] ¹⁴
	\$2,478,043	\$1,060,774	\$1,098,276	\$4,637,093
✓ (partial) ¹¹	\$300,000	\$600,000	\$651,877	\$1,551,877
✓	\$470,000	\$755,987	\$800,677	\$2,026,664
	0	\$755,987	\$800,677	\$1,556,664
	\$2,307,808	\$1,648,250	\$1,656,999	\$5,613,057
✓ (partial) ¹¹	\$3,149,637 ¹⁵	\$1,060,774	\$1,098,276	\$5,308,687
✓*	\$1,211,326	\$755,987	\$800,677	\$2,767,990 [\$2,093,000] ¹⁶
✓	\$925,026	\$755,987	\$800,677	\$2,481,690
✓	\$1,003,087 ¹⁷	\$755,987	\$800,677	\$2,559,751
	0	\$1,060,774	\$1,098,276	\$2,159,050
	\$1,023,911	\$755,987	\$800,677	\$2,580,575
	\$1,138,000	\$755,987	\$800,677	\$2,694,664 [\$5,872,000] ¹⁸
✓ (partial) ¹¹	\$1,609,635	\$1,060,774	\$1,098,276	\$3,768,685
✓ (partial) ¹¹	\$2,495,000	\$1,060,774	\$1,098,276	\$4,654,050
✓	\$694,060	\$755,987	N/A	\$1,450,047
✓ ¹¹	\$17,718,424 ¹⁹	\$755,987	\$800,677	\$19,275,088
✓	\$548,293	\$755,987	\$800,677	\$2,104,957
✓	0	\$600,000	N/A	\$600,000
	\$687,188	\$755,987	\$800,677	\$2,243,852
	\$2,893,607 ²¹	\$755,987	\$800,677	\$4,450,271
	0	\$755,987	\$800,677	\$1,556,664
✓ ¹¹	\$1,287,489	\$1,060,774	\$1,098,276	\$3,446,539
	\$500,000	\$755,987	\$800,677	\$2,056,664
✓ (NYC only)	\$2,255,748	\$1,648,250	\$1,656,999	\$5,560,997
	\$1,799,000	\$1,060,774	\$1,098,276	\$3,958,050
✓*	\$500,000	\$600,000	\$651,877	\$1,751,877
✓ ¹¹	0	\$600,000	\$651,877	\$1,251,877
✓ ¹¹	\$1,200,000	\$1,060,774	\$1,098,276	\$3,359,050
✓	0	\$755,987	N/A	\$755,987
✓ ¹¹	\$1,169,678	\$755,987	\$800,677	\$2,726,342
✓ (partial) ¹¹	\$2,042,800	\$1,060,774	\$1,098,276	\$4,201,850
	\$300,000	\$600,000	\$651,877	\$1,551,877
✓ ¹¹	\$500,000	\$600,000	\$651,877	\$1,751,877
	\$500,000	\$755,987	\$800,677	\$2,056,664
✓*	\$300,000	\$600,000	\$651,877	\$1,551,877
	\$694,060	\$755,987	\$800,677	\$2,250,724
	\$3,200,000	\$1,648,250	\$1,656,999	\$6,505,249
	\$300,000	\$600,000	\$651,877	\$1,551,877
✓	\$1,006,418	\$755,987	\$800,677	\$2,563,082
	\$500,000	\$600,000	\$651,877	\$1,301,877
	\$2,660,252	\$1,060,774	\$1,098,276	\$4,819,302
	0	\$1,060,774	\$1,098,276	\$2,159,050
	\$500,000	\$755,987	\$800,677	\$2,056,664
	\$2,071,063 ²²	\$755,987	\$800,677	\$3,627,727 ²³
	\$500,000	\$600,000	\$651,877	\$1,751,877

Center for Immigration Studies

Driver License Security Implementation: Notes

¹ Data compiled by the Coalition for a Secure Driver's License, see <http://www.secure-license.org/>.

² CDLIS-Commercial Driver's License Information System administered by American Association of Motor Vehicle Administrators (AAMVA), alongside the National Driver Registry.

³ SSOIV-Social Security On-Line Verification administered by the Social Security Administration.

⁴ SAVE-Systematic Alien Verification for Entitlements developed by the US Citizenship and Immigration Services Agency of DHS and administered by AAMVA.

⁵ EVVE-Electronic Verification of Vital Events developed by the National Association for Public Health Statistics and Information Systems (NAPHSIS).

⁶ In FY08, DHS awarded competitive grants with priority to states seeking to be the "hub" for ID verification networking among the states and with the federal government. This used a combined pool of 2005 and 2007 funding for the Driver License Security Grant Program created under the REAL ID law.

⁷ In FY09 and FY10, DHS is conducting a two-part grant process per total of \$100M (\$50M more than the 2007 funding) allocated under the Consolidated Security, Disaster Assistance and Continuing Appropriations Act of 2009. These were noncompetitive grants based on licenses issued in state. There was a decision to forego allocation as a competitive process awarding to states for proposals "that improve state capabilities consistent with the requirements of the REAL ID rule."

⁸ Alabama Department of Public Safety, "Special Report on the State's Compliance with Public Law 109-13" (July 25, 2008). Data obtained by the Coalition for a Secure Driver's License.

⁹ To receive a competitive grant from DHS in FY08, states had to submit a grant proposal stating how the funding would be used for REAL ID implementation. States that failed to submit a proposal did not receive funding.

¹⁰ Connectivity information was unavailable for U.S. jurisdictions Am. Samoa, Guam, N. Mariana Islands, Puerto Rico and U.S. Virgin Islands.

¹¹ New since January 2009; (partial) = in the process of implementation now.

¹² Jennifer Cohan, Director, Delaware Division of Motor Vehicles, AMMVA Region/Annual Conference Presentation (July 25, 2008). Obtained by Coalition for a Secure Driver's License.

¹³ Of this amount, Florida received \$1.2M to partner with the lead hub State Mississippi for pilot implementation and verification testing.

¹⁴ Florida Department of Highway Safety and Motor Vehicles, "Fiscal Year 2009-2010 Legislative Budget Request" (Sept. 22, 2008). Data obtained by Coalition for a Secure Driver's License.

¹⁵ Of this amount, Indiana received \$1.2M to partner with the lead hub State Mississippi for pilot implementation and verification testing.

¹⁶ "Iowa- An Act Relating to and Making Transportation and Other Infra-Structure-related Appropriations to the Department of Transportation" (2009): "Motor vehicles:

3 20 \$ 1,555,005

3 21 FTEs 498.00

3 22 Of the total amount appropriated in this paragraph and the

3 23 total full-time equivalent positions authorized in this

3 24 paragraph, the expenditure of \$1,148,000 and the filling of 20

3 25 full-time equivalent positions are contingent upon the need of

3 26 the department for the additional positions in order to

3 27 implement federal requirements pursuant to the federal REAL ID

3 28 Act of 2005 and successor legislation."

[http://search.legis.iowa.us/NXT/gateway.dll/clf/Current%20Legislation/enrolled/2009/hf/hf805?f=templates\\$fn=document-frameset.htm&q=\[rank%3A\[sum%3A\[orderedprox,0%3A\[stem%3Areal\]\] \[stem%3Aid\]\]\]\]\\$x=server\\$3.0#LPHit1](http://search.legis.iowa.us/NXT/gateway.dll/clf/Current%20Legislation/enrolled/2009/hf/hf805?f=templates$fn=document-frameset.htm&q=[rank%3A[sum%3A[orderedprox,0%3A[stem%3Areal]] [stem%3Aid]]]]$x=server$3.0#LPHit1)

¹⁷ In a separate grant for EVVE, Kentucky received was awarded a \$3M pilot grant in Dec. 2006. The purpose of the grant was to prepare for the nationwide deployment of electronic birth record verification.

¹⁸ "Maryland Motor Vehicle Administration Capital Program Summary," (FY09 Total Accumulated Expenditures to comply with "The Real ID Act").

¹⁹ Mississippi received \$17M as lead state for verification hub requirements and development.

²⁰ States with laws prohibiting REAL ID implementation.

²¹ Of this amount, Nevada received \$1.2M to partner with the lead hub State Mississippi for pilot implementation and verification testing.

²² Of this amount, Wisconsin received \$1.2M to partner with the lead hub State Mississippi for pilot implementation and verification testing.

²³ The Wisconsin Legislature allocated \$9.8 million for FY 2008 and \$12.2 million for FY 2009 to assure REAL ID compliance. Legislative Reference Bureau, "Wisconsin Briefs No. 08-3 REAL ID" (March 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H. STATE LAWS OPPOSING REAL ID⁵¹¹

State Legislative Activity in Opposition to the Real ID January 2014

Statutory Opposition to Comply with the Real ID	Approved Concurrent or Joint Resolutions in Opposition to the Real ID ¹
Alaska - 2008 SB 202, 2013 HB 69 Arizona - 2008 HB 2677; 2009 HB 2426	Arkansas - 2007 SCR 16, SCR 22 Colorado - 2007 HJR 1047
Georgia ² - 2007 SB 5 Idaho - 2008 HB 606	Hawaii - 2007 SCR 31 Illinois - 2007 HJR 27
Louisiana - 2008 HB 715	Nebraska - 2007 LR 28
Maine - 2007 LD 1138	Nevada - 2007 AJR 6
Minnesota - 2009 HB 988	North Dakota - 2007 SCR 4040
Missouri ³ - 2009 HB 361	South Dakota - 2008 SCR 7
Montana - 2007 HB 287	
New Hampshire - 2007 HB 685	
Oklahoma - 2007 SB 464	
Oregon ⁴ 2009 SB 536	Approved House or Senate Resolutions in Opposition to the REAL ID
Pennsylvania 2012 SB 354	Michigan - 2007 HR 176
South Carolina - 2009 SB 449	Pennsylvania - 2008 HR 767, SR 126
Utah - 2010 HB 234	
Virginia ⁵ - 2009 HB 1587, SB 1431	
Washington ⁶ - 2007 SB 5087	

¹ Does not include states that have adopted both statutes and resolutions in opposition to the Real ID. Those states are only listed as states adopting statutes in opposition to the REAL ID.

² Allows the Governor to delay Real ID compliance until the U.S. Department of Homeland Security guarantees that defined safeguards will protect the economic and biological privacy of the citizens of Georgia.

³ Prohibits the Department of Revenue from amending procedures for applying for a driver's license or identification card in order to comply with the goals or standards of the federal Real ID Act of 2005, any rules or regulations promulgated under the authority granted in such act, or any requirements adopted by the American Association of Motor Vehicle Administrators for furtherance of the act. Contains other provisions regarding driver's licenses and identification cards

⁴ Became law without the Governor's signature. Prohibits any state agency from expending any funds to implement the Real ID Act unless the state DOT implements sufficient measures to protect individuals privacy, and puts safeguards in place that protect against the unauthorized disclosure or use of an individual's personal identifying information. The DOT cannot participate in the Real ID Act if it: requires the department to participate in any multistate or federal shared database program unless the department is able to provide sufficient security measures to protect the privacy of individuals; charges unreasonable fees; or places unreasonable record keeping burdens on an applicant for issuance, renewal or replacement of a driver license, driver permit or identification card. Requires the state DOT to prepare a report that analyzes the cost to the state of the Real ID Act.

⁵ Prohibits implementation to comply with any provision of the Real ID Act and with any other federal law, regulation, or policy that would compromise the economic privacy, biometric data or biometric samples of any resident of the Commonwealth.

⁶ Prohibits implementation unless changes are made regarding privacy and funding.

Source: National Conference of State Legislatures, January 2013

⁵¹¹ "National Conference of State Legislatures, "The REAL ID: State Legislative Activity in Opposition to REAL ID," 23.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- ACLU-NJ. "State Settles ACLU-NJ Lawsuit by Agreeing to Drop TRU-ID Program." October 5, 2012. <http://www.aclu-nj.org/news/2012/10/05/drop-tru-id-program>.
- Adams, Glenn, and The Associated Press. "Maine Says No Thanks to ID Act; U.S. Law Cumbersome, Costly Says Lawmakers." *The Bangor Daily News*, Accessed December 30, 2013. <http://archive.bangordailynews.com/2007/01/26/maine-says-no-thanks-to-id-act-u-s-law-cumbersome-costly-says-lawmakers/>.
- American Association of Motor Vehicle Administrators, The. "2012 State Status of Real ID." August 2, 2012. <http://www.aamva.org/>.
- Baker, Stewart. Assistant Secretary for Policy. "Real ID." March 20, 2008, *DHS Leadership Journal Archive*. <http://ipv6.dhs.gov/journal/leadership/labels/Real%20ID.html>.
- Bangor Daily News, The. "Driver's License Fix." Accessed December 29, 2013. <http://archive.bangordailynews.com/2008/02/25/drivers-license-fix/>.
- . "Dunlap Named to Serve on Federal Committee." Accessed March 8, 2014. <http://archive.bangordailynews.com/2005/04/14/dunlap-named-to-serve-on-federal-committee/>.
- . "License Failures." Accessed December 29, 2013. <http://archive.bangordailynews.com/2008/04/09/license-failures/>.
- . "Revisit Real ID." Accessed December 30, 2013. <http://bangordailynews.com/2009/04/30/opinion/revisit-real-id/>.
- Bass, Brendon. "What Is an PDF417 Barcode." *Am Labels*, December 15, 2010. <http://www.support-amlabels.co.uk/2010/11/what-is-an-pdf417-barcode>.
- BBC. "In Full: Smith ID Card Speech." sec. UK Politics, March 6, 2008. http://news.bbc.co.uk/2/hi/uk_news/politics/7281368.stm.
- . "UK's National ID Card Unveiled." sec. UK Politics, July 30, 2009. <http://news.bbc.co.uk/2/hi/8175139.stm>.
- Bennett, Colin J., and David Lyon. *Playing The Identity Card: Surveillance, Security and Identification in Global Perspective*. New York: Routledge, 2008. <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=529287>.

- Breckenridge, Keith. "The Elusive Panopticon: The HANIS Project and the Politics of Standards in South Africa." In *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, edited by Colin J. Bennett and David Lyon. London; New York: Routledge, 2008.
- Bruno, Joseph F. MVC Custodian of Records. Office of Legal and Regulatory Affairs. *New Jersey Response to ACLU Open Public Records Act Request*, April 24, 2012.
- BusinessDictionary.com. "What Is Unfunded Mandate? Definition and Meaning." Accessed December 16, 2013. <http://www.businessdictionary.com/definition/unfunded-mandate.html>.
- Carafano, James Jay, Ph.D. "Web Memo: DHS Gets REAL ID Right." *The Heritage Foundation*, February 7, 2008. <http://www.heritage.org/research/reports/2008/02/dhs-gets-real-id-right>.
- Center for Immigration Studies. "Repealing REAL ID? Rolling Back Driver's License Security (Announcement)." Accessed September 3, 2013. <http://www.cis.org/realidannounce>.
- . "Update on Digitization of Vital Records." Accessed February 5, 2014. <http://cis.org/kephart/evve-update>.
- Clarke, Roger A. "Human Identification in Record Systems" (June 1989).
- . "National Identity Schemes—Elements." February 8, 2006. <http://www.rogerclarke.com/DV/NatIDSchemeElms.html>.
- . "The Resistible Rise of the National Personal Data System." *Software L. J.* 29, 33–36 (1992).
- Coalition for a Secure Driver's License. "About Us." Accessed February 13, 2014. <http://www.secure-license.org/about-us>.
- Delaware Department of Transportation. "Press Release: Division of Motor Vehicles Receives Award for Outstanding Fraud Protection of State Residents." May 29, 2012. <http://www.deldot.gov/home/newsroom/release.shtml?id=4370>.
- . "Press Release: DMV Announces New Secure Driver License and Identification Card System." April 13, 2009. <http://www.deldot.gov/public.ejs?\command=PublicNewsDisplay&id=3324>.
- Denison, Doug. "Delaware DMV Unveils New Secure ID Cards." *Middletown Transcript*, June 16, 2010. <http://www.middletowntranscript.com/apps/pbcs.dll/article?avis=DE>.

———. “Newsmaker Q&A: Jennifer Cohan, Director of the Delaware Division of Motor Vehicles.” *Dover Post*, August 24, 2010. <http://www.doverpost.com/apps/pbcs.dll/article?avis=DE>.

Department of Homeland Security. “DHS Determines 13 States Meet REAL ID Standards.” Accessed December 2, 2013. <http://www.dhs.gov/news/2012/12/20/dhs-determines-13-states-meet-real-id-standards>.

———. *DHS Press Release: Remarks by Homeland Security Secretary Michael Chertoff at Pen and Pad Briefing on the Department’s Fifth Anniversary*, March 6, 2008.

———. “DHS Releases Phased Enforcement Schedule for REAL ID.” Accessed December 29, 2013. <http://www.dhs.gov/news/2013/12/20/dhs-releases-phased-enforcement-schedule-real-id>.

———. *DHS Releases REAL ID Regulation*, January 11, 2008.

———. “Final Rule, Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. 5271.” January 29, 2008. <http://www.gpo.gov/fdsys/pkg/FR-2008-01-29/html/08-140.htm>.

———. *Final Rule: Privacy Impact Assessment*, January 11, 2008.

———. *Notice of Proposed Rulemaking: Privacy Impact Assessment*, March 1, 2007.

———. *Privacy Impact Assessment for the REAL ID Act: In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, March 1, 2007.

———. *Privacy Impact Assessment for the REAL ID Final Rule*, January 11, 2008.

———. “REAL ID Enforcement in Brief.” December 20, 2013. <http://www.dhs.gov/sites/default/files/publications/REAL-ID-IN-Brief-20131220.pdf>.

———. *Regulatory Evaluation Final Rulemaking 6 CFR Part 37*, January 17, 2008.

———. *Secure Identification State Progress: Fiscal Year 2012 Report to Congress*, August 28, 2012, 15 citing *REAL ID Act* Section 202(c)(3)(A).

Department of Justice. “Department of Transportation, Notice of Proposed Rulemaking: State Issued Driver’s Licenses Minimum Standards for Driver’s Licenses and Comparable Identification Documents, 63 Fed Reg. 33,220.” June 17, 1998. http://www.justice.gov/eoir/vll/fedreg/1998_1999/fr17jn98P.pdf.

- “Department of Homeland Security, Notice of Proposed Rulemaking: Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed Reg. 10,819.” Washington, DC: GPO, 2007. <http://www.gpo.gov/fdsys/pkg/FR-2007-03-09/html/07-1009.htm>.
- “Department of Transportation, Withdrawal of Proposed Rule on State-Issued Driver’s Licenses and Comparable Identification Documents 66 Fed Reg, 56261.” Washington, DC: GPO, 2001. <http://www.gpo.gov/fdsys/pkg/FR-2001-11-07/html/01-28007.htm>.
- Dershowitz, Alan. “Thinking About National ID Cards.” May 2002. <http://triton.towson.edu/~swartout/cosc311/dershowitz2.htm>.
- Dilger, Robert Jay, and Richard S. Beth. “Unfunded Mandates Reform Act: History, Impact, and Issues.” 2013. <http://www.fas.org/sgp/crs/misc/R40957.pdf>.
- Division of Libraries’ Blog. “Q: ‘What Is a Federally Compliant Delaware Driver’s License (and ID)?.’” Accessed December 23, 2013. <http://library.blogs.delaware.gov/2012/10/07/federally-compliant-de-drivers-license/>.
- Douglas, Governor James H., and Governor Joe Manchin III. *National Governor’s Association Letter to Congress Urging Enactment of PASS ID Legislation*, November 18, 2009.
- Easesoft.net. “PDF417 Symbology.” February 24, 2013. <http://www.easesoft.net/PDF417.html>.
- Editorial Board. “The Case for a National ID Card.” *The Washington Post*, sec. Opinions, February 2, 2013. http://www.washingtonpost.com/opinions/the-case-for-a-national-id-card/2013/02/02/49d4fb80-6cb5-11e2-ada0-5ca5fa7ebe79_story.html.
- Egelman, Serge, and Lorri Faith Cranor. “The REAL ID Act: Fixing Identity Documents With Duct Tape.” *I/S A Journal of Law and Policy* 2, no. 1 (2006).
- Electronic Frontier Foundation. “Success Story: Dismantling UK’s Biometric ID Database.” Accessed August 25, 2013, <https://www EFF.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database>.
- Electronic Privacy Information Center. *REAL ID Implementation Review: Few Benefits, Staggering Costs: Analysis of the Department of Homeland Security’s National ID Program*, May 2008.
- Federal Emergency Management Administration. *Grant Programs Directorate Information Bulletin No. 277 January 28, 2008: Consolidation of Fiscal Year (FY) 2008 REAL ID Funding Availability*, January 28, 2008.

- Federation for Immigration Reform. "Identity and Immigration Status of 9/11 Terrorists (2011)." November 2011. <http://www.fairus.org/issue/identity-and-immigration-status-of-9-11-terrorists>.
- Finklea, Kristin M. *Identity Theft: Trends and Issues*. CRS Report R40599. Washington, DC: Congressional Research Service, February 15, 2012.
- Frassinelli, Mike. "N.J. Drops Plan to Require Extra Documents to Get Driver's License." Accessed September 14, 2013. http://blog.nj.com/ledgerupdates_impact/print.html?entry=/2012/10/nj_drops_plan_to_require_addit.html.
- Froomkin, A. Michael. "The Uneasy Case for National ID Cards." In *Securing Privacy in the Internet Age*, edited by A. Chander, L. Gelman, M. J. Radin. 295–321. Stanford: Stanford Law Books, 2008.
- Frum, David, and Richard Norman Perle. *An End to Evil: How to Win the War on Terror*. New York: Ballantine, 2004.
- Garcia, Michael J., Margaret M. Lee, and Todd Tatelman. *Immigration: Analysis of the Major Provisions of the REAL ID Act of 2005*. Washington, DC: Congressional Research Service, May 25, 2005. 38. <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA453701>.
- Gates, Kelly. "The United States REAL ID Act and the Securitization of Identity." In *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, edited by Colin J Bennett and David Lyon. London; New York: Routledge, 2008.
- Google Images. "PDF 417 2D Stacked Barcode." Accessed March 4, 2013. https://www.google.com/search?q=PDF+417&rlz=1C1CHMO_enUS580US580&espv=210&tbm=isch&tbo=u&source=univ&sa=X&ei=zE4tU_j9E8na2QWDh4HwDw&ved=0CD0Q7Ak&biw=1024&bih=724#q=google+images+PDF+417+2D+Stacked+Barcode&tbm=isch.
- Government Printing Office. "Federal Register, Volume 76 Issue 44 Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes." March 7, 2011. <http://www.gpo.gov/fdsys/pkg/FR-2011-03-07/html/2011-5002.htm>.
- Harrell, Erika, and Lynn Langton. "Victims of Identity Theft, 2012." *Bureau of Justice Statistics*, December 2013. <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.
- Heritage Foundation, The. "REAL ID Realities: Perspectives on the Future of the REAL ID Program." Accessed February 1, 2014. <http://www.heritage.org/events/2013/01/real-id>.

- Home Office. "Commencement of the Identity Cards Act 2006—Issue of Identity Cards and New Criminal Offences—Publications—GOV.UK." Accessed August 25, 2013, <https://www.gov.uk/government/publications/commencement-of-the-identity-cards-act-2006-issue-of-identity-cards-and-new-criminal-offences>.
- . "ID Cards No Longer Valid—News Stories—GOV.UK." January 21, 2011, <https://www.gov.uk/government/news/id-cards-no-longer-valid>.
- Honolulu Star-Advertiser. "State Driver's Licenses, ID Cards Do Not Conform to Federal." Accessed February 16, 2014. http://www.staradvertiser.com/news/20110428_State_drivers_licenses_ID_cards_do_not_conform_to_federal_rules.html.
- Institute for Communitarian Policy Studies, The. George Washington University. "Communitarian Update #48» Institute for Communitarian Policy Studies." September 24, 2002. <http://icps.gwu.edu/contact/mailling-list/communitarian-letter-archives/communitarian-update-48/>.
- Jacobs, Marine. "Smart ID Card Rollout Underway." *DefenceWeb*, August 26, 2013. http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=31673:smart-id-card-rollout-underway&catid=54:Governance&Itemid=118.
- Kent, Stephen T. et al. *IDs--Not That Easy Questions about Nationwide Identity Systems*. Washington, DC: National Academy Press, 2002. <http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=87005>.
- Kephart, Janice. "REAL ID Final Rules: A Summary." *Center for Immigration Studies*, March 2008.
- . "REAL ID Implementation: Less Expensive, Doable, and Helpful in Reducing Fraud." *Center for Immigration Studies*, January 2011. <http://cis.org/real-id>.
- . "Repealing REAL ID? Rolling Back Driver's License Security." *Backgrounder*, *Center for Immigration Studies*, June 2009.
- . "The Appearance of Security, REAL ID Final Regulations vs. Pass ID Act of 2009." *Backgrounder*, *Center for Immigration Studies*, April 2009.
- Langton, Lynn, and Michael Planty. *Victims of Identity Theft, 2008*. National Crime Victimization Survey, Bureau of Justice Statistics, December 2010.
- Leary, Mal, and Capitol News Service. "Maine Receives \$1M Real ID Grant." *The Bangor Daily News*, accessed February 24, 2014. <http://archive.bangor-dailynews.com/2008/06/24/maine-receives-1m-real-id-grant/>.

- Mail Online. "India's Identity Crisis: Between Aadhaar, Passport, PAN and NPR, Why Are We Still Struggling to Prove Our Identities?." March 22, 2013. <http://www.dailymail.co.uk/indiahome/indianews/article-2297714/Indias-identity-crisis-Between-Aadhaar-passport-PAN-NPR-struggling-prove-identities.html>.
- Maine Department of Secretary of State. *Report of the Working Group Convened by the Secretary of State to Examine Laws Governing Eligibility and Documentation Requirements for Driver's Licenses and Non-Driver Identification Cards*, December 5, 2007.
- Maine State Legislature. "An Act to Enhance the Security of State Credentials, Maine Revised Statutes Annotated." 2008. <http://www.mainelegislature.org>.
- . "An Act to Protect the Privacy of Maine Residents Under the Driver's License Laws, Maine Revised Statutes Annotated." 2011. http://www.mainelegislature.org/legis/bills/display_ps.asp?paper=HP0803&PID=1456&snum=125&sec0.
- . "Summary of LD 1068 (HP 803): An Act To Protect the Privacy of Maine Residents under the Driver's License Laws." Accessed January 19, 2014. <http://www.mainelegislature.org/LawMakerWeb/summary.asp?LD=1068&SessionID=9>.
- McCoy, Kevin. "Identity Thieves Tax the System." *USA Today*, April 10, 2008.
- Mehmood, Taha. "India's New ID Card: Fuzzy Logics, Double Meanings and Ethnic Ambiguities." In *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, edited by Colin J Bennett and David Lyon. London; New York: Routledge, 2008.
- Meingast, Marci, Jennifer King, and Deirdre K. Mulligan. "Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. E-Passport." In *RFID, 2007. IEEE International Conference on RFID, 2007*. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4143504.
- Minner, Governor Ruth Ann. *Will REAL ID Actually Make Us Safer: Privacy and Civil Liberties Hearing May 2007*. Washington, DC, 2007.
- NAPHSIS. "EVVE." Accessed February 5, 2014. <http://www.naphsis.org/Pages/EVVE.aspx>.
- National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Authorized Edition. Westminster, MD: SOHO Books, as released by the U.S. Government, 2010.
- . *9/11 and Terrorist Travel: A Staff Report of the National Commission on Terrorist Attacks upon the United States*. Franklin, TN: Hillsboro Press, 2004.

- National Conference of State Legislatures. "NCSL IN DC, Task Forces, Policies Natural Resources and Infrastructure." Accessed December 15, 2013. <http://www.ncsl.org/ncsl-in-dc/task-forces/policies-natural-resources-and-infrastructure.aspx#realid>.
- . "The REAL ID: State Legislative Activity in Opposition to REAL ID." June 2012. <http://www.ncsl.org/documents/standcomm/sctran/REALIDComplianceReport.pdf>.
- National Governor's Association. "National Governor's Association Statement on Passage of REAL ID." May 12, 2005. http://www.nga.org/cms/home/news-room/news-releases/page_2005/col2-content/main-content-list/title_nga-statement-on-passage-of-real-id.html.
- . National Conference of State Legislatures, and American Association of Motor Vehicle Administrators. *The REAL ID Act: National Impact Analysis*. September 2006.
- Nelson, Lisa S. *America Identified: Biometric Technology and Society*. Cambridge, MA: The MIT Press, 2011. <http://books.google.com/books?id=64zo8GjybdYC&printsec=frontcover&dq=America+Identified&hl=en&sa=X&ei=k7cRUtKnEKugyAHy3IEo&ved=0CC8Q6AEwAA#v=onepage&q=America%20Identified&f=false>.
- New Jersey State Police. "2011 News Release: 17 Guns Seized, 13 Arrested in Co-Op Cases Involving Gun Running, Carjacking, Drug Dealing, and Supplying Fraudulent IDs." April 14, 2011. <http://www.njsp.org/news/pr041411.html>.
- New York Civil Liberties Union. *No Freedom Without Privacy: The Real ID Act's Assault on Americans' Everyday Life*, February 2009.
- News Journal, The*. "DMV Must Get a Handle on Real ID to Ease Delays." July 24, 2010, LexisNexis Academic.
- . "Proposed Changes in Secured ID Could Make Law More Workable." October 20, 2009, LexisNexis Academic.
- . "Real ID Has So Many Pitfalls And Not Enough Money To Back It Up." May 28, 2008, LexisNexis Academic.
- Noack, Torsten, and Herbert Kubicek. "The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany." *Identity in the Information Society* 3, no. 1 (March 25, 2010): 87–110, doi:10.1007/s12394-010-0051-1.
- Nogueira, Monica, and Noel Greis. "Uses of RFID Technology in U.S. Identification Documents." *University of North Carolina, Center for Logistics and Digital Strategy*, 2009.

- Noore, Afzel, Nikhil Tungala, and Max M. Houck. "Embedding Biometric Identifiers in 2D Barcodes for Improved Security." *Computers and Security* 23, no. 8 (December 2004).
- Ofer, Udi, Ari Rosmarin, and Michael Cummings. *No Freedom Without Privacy: The REAL ID Act's Assault on Americans' Everyday Life*. NY ACLU, February 2009.
- Office of the Inspector General, Social Security Administration. "Audit Report: The Social Security Administration's Compliance With Intelligence Reform and Terrorism Prevention Act of 2004 Provisions Regarding Security of Social Security Cards and Numbers." May 2008. <http://oig.ssa.gov/sites/default/files/audit/full/html/A-08-08-18058.html>.
- Open States. "Bill Text-HP 803-Maine 125th Legislature (2011–2012)." Accessed January 29, 2014. <http://openstates.org/me/bills/125/HP803/documents/MED00003463/>.
- Perlman, Bruce J. "Governance Challenges and Options for State and Local Governments." *State and Local Government Review* 42, no. 3 (December 1, 2010): 246–257. doi:10.1177/0160323X10390050.
- Pollways. "Democrat Dunlap Declares." Accessed March 8, 2014. <http://pollways.bangordailynews.com/2011/11/02/national/democrat-dunlap-declares/>.
- President's Identity Theft Task Force, The. *Combating Identity Theft: A T Strategic Plan*, April 2007, 43.
- Pushkarna, Neha. "India's Identity Crisis: Between Aadhaar, Passport, PAN and NPR, Why Are We Still Struggling to Prove Our Identities? Capital Hopes to Do Everything with Aadhaar." *Mail Online*, March 22, 2013. <http://www.dailymail.co.uk/indiahome/indianews/article-2297714/Indias-identity-crisis-Between-Aadhaar-passport-PAN-NPR-struggling-prove-identities.html>.
- Record, The*. "A License for Trouble and a Boon for Identity Theft." May 6, 2005, LexisNexis Academic; see also, *The Star-Ledger*. "The Party of Centralized Power" July 19, 2005, LexisNexis Academic.
- . "The REAL ID Solution: Are You Who You Say You Are?" January 16, 2008, LexisNexis Academic.
- . "REAL ID Enforcement Begins in 2014, 21 States Compliant." December 20, 2013. <http://www.reuters.com/article/2013/12/20/csdl-dhs-real-id-act-idUSnPnDCfLrqh+168+PRN20131220>.

- Rolph, C. H. "The English Identity Cards." In *National Identification Systems: Essays in Opposition*, edited by Carl Watner and Wendy McElroy. Jefferson, NC: McFarland & Co., 2004.
- Senate Committee on Appropriations. *Senate Report 112-74*, September 7, 2011, 11.
- Sharma, Amol. "India Launches Project to ID 1.2 Billion People." *Wall Street Journal*, sec. Technology, September 29, 2010. <http://online.wsj.com/article/SB10001424052748704652104575493490951809322.html>.
- Singh, Hardeep Guide. "Role of Biometric Technology in AADHAR Enrollment." January 21, 2012. <http://dspace.thapar.edu:8080/dspace/handle/10266/1734>.
- Star Ledger, The. "Revoke This License Plan New Jersey Should Back Out of Federal ID Program." May 14, 2012, LexisNexis Academic.
- . "Revoke Driver's License Law." March 4, 2007, LexisNexis Academic.
- State of Delaware Division of Motor Vehicles. "Graduated Driver License." Accessed July 9, 2013. http://www.dmv.de.gov/services/driver_services/drivers_license/dr_lic_secure_dl_get_started.shtml.
- State of Delaware. "Delaware Department of Transportation—Divisions." Accessed July 9, 2013. <http://www.deldot.gov/home/divisions/>.
- . "Delaware Department of Transportation—Secretary." Accessed January 31, 2014. <http://www.deldot.gov/home/secretary/>.
- . "State of Delaware Division of Motor Vehicles—About DMV." Accessed July 9, 2013. <http://www.dmv.de.gov/>.
- . DelDOT Newsroom. *Press Release: The American Association of Motor Vehicle Administrators Welcomes Delaware Director of DMV as Chairwoman of the International Board of Directors*, September 4, 2013.
- State of Maine. "Maine Rejects Real ID Act: Joint Resolution Refutes Plan for National Identification Cards." January 25, 2007. <http://www.maine.gov/sos/news/2007/RealIDAct.html>.
- . "Obtaining a Driver's License." Accessed March 8, 2014. <http://www.maine.gov/sos/bmv/licenses/getlicense.html>.
- . "Secretary Dunlap Details New Requirements for Issuing Driver Licenses and State ID Cards." November 14, 2008. <http://www.maine.gov/sos/news/2008/new-dl-requirements.htm>.

- . “Secretary of State Matt Dunlap Reminds Motorists of Requirements for Obtaining Driver Licenses and State ID Cards.” May 7, 2009. <http://www.maine.gov/sos/news/2009/legal-presence-reminder.htm>.
 - . “Secretary of State Matt Dunlap Takes Oath for Third Term.” Accessed February 23, 2014. <http://www.maine.gov/sos/news/2009/sosthirdterm.htm>.
 - . “Secretary of State Summers Reveals Newly Designed Driver’s License and Identification Cards.” March 22, 2011. <http://www.maine.gov/sos/news/2011/newdriverlicense.htm>.
 - . Department of the Secretary of State. “Maine Civil Liberties Union Award.” January 11, 2008. <http://www.maine.gov/sos/news/2008/MaineCivil.html>.
- State of New Jersey. “New Jersey 6 Point ID Brochure.” June 14, 2013. http://www.state.nj.us/mvc/pdf/Licenses/ident_ver_posterpint.pdf.”
- . “Press Release: Attorney General & MVC Chief Announce New Charges Resulting From High-Tech Program ‘Operational Facial Scrub’ to Detect False Driver’s Licenses.” February 20, 2014. <http://www.state.nj.us/mvc/PressReleases/archives/2014/022014a.htm>.
- State of New Jersey. Motor Vehicle Commission. “6 Point ID Verification.” Accessed February 8, 2014. <http://www.state.nj.us/mvc/Licenses/6PointID.htm>.
- . “Chief Administrator.” Accessed March 2, 2014. <http://www.state.nj.us/mvc/About/ChiefAdministrator.htm>.
 - . “Media Release: Christie Administration Announces New ‘Skip the Trip’ Drivers License and ID Mail Renewal Service for New Jerseyans New Process to Aid Implementation of Federal REAL ID Standards.” April 2, 2012. <http://www.state.nj.us/mvc/PressReleases/archives/2012/040212.htm>.
 - . “MVC Honored with National Security Excellence Award.” October 5, 2011. <http://www.state.nj.us/mvc/PressReleases/archives/2011/100511.htm>.
 - . “NJ Motor Vehicle Chief, Attorney General and Homeland Security Director Unveil the State’s New, More Secure Driver License.” May 11, 2011. <http://www.state.nj.us/mvc/PressReleases/archives/2011/051111.htm>.
 - . “TRU-ID Requirements Delayed Due to ACLU Court Motion.” *Noodls*. Accessed January 12, 2014. <http://www.noodls.com/viewNoodl/14226686/state-of-new-jersey-motor-vehicle-commission/tru-id-requirements-delayed-due-to-aclu-court-motion>.
 - . “TRU-ID.” Accessed February 8, 2014. <http://www.state.nj.us/mvc/Licenses/truid.htm>.

- . “What Is the MVC?.” Accessed February 23, 2014. <http://www.state.nj.us/mvc/About/AboutMVC.htm>.
- Steinbock, Daniel J. “Fourth Amendment Limits on National Identity Cards.” In *Privacy and Technologies of Identity: A Cross-disciplinary Conversation*, edited by Katherine Jo Strandburg and Daniela Stan Raicu, CIPLIT Symposium on Privacy and Identity: The Promise and Perils of a Technological Age. New York: Springer Science+Business Media, 2006.
- Tatelman, Todd B. “Intelligence Reform and Terrorism Prevention Act of 2004: National Standards for Drivers’ Licenses, Social Security Cards, and Birth Certificates.” January 6, 2005. <http://www.fas.org/irp/crs/RL32722.pdf>.
- Treasury Inspector General for Tax Administration. *Substantial Changes Are Needed to the Individual Taxpayer Identification Number Program to Detect Fraudulent Applications*. Washington, DC, July 16, 2012). <http://www.treasury.gov/tigta/auditreports/2012reports/201242081fr.html>.
- U.S. Government Accountability Office. *Counterfeit Documents Used to Enter the United States from Certain Western Hemisphere Countries Not Detected*. GAO-03-713T. 2003. <http://www.gao.gov/products/GAO-03-713T>.
- . *Driver’s License Security: Federal Leadership Needed to Address Remaining Vulnerabilities*, GAO-12-893. 2012.
- . *Firearms: Purchased from Federal Firearms Licensees Using Bogus Identification*. GAO-01-427NI. 2001. <http://www.gao.gov/products/577970>.
- . *Purchase of Firearms Using a Counterfeit Federal Firearms License*. GAO-02-383RNI. 2002. <http://www.gao.gov/products/GAO-02-383RNI>.
- . *Security: Breaches at Federal Agencies and Airports*. GAO/T-OSI-00-10. 2000. <http://www.gao.gov/products/T-OSI-00-10>.
- . *Security Breaches at Federal Buildings in Atlanta, Georgia*. GAO-02-668T. 2002. <http://www.gao.gov/products/GAO-02-668T>.
- . *Social Security Numbers: Ensuring the Integrity of the SSN*. GAO-03-641T. 2003. <http://www.gao.gov/assets/120/110152.pdf>.
- . *Social Security Numbers: Increased SSN Verification and Exchange of States’ Driver Records Would Enhance Identity Verification*. GAO-03-920. 2003. <http://www.gao.gov/assets/240/239643.pdf>.
- . *Testimony Before the Senate Committee on Finance, Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*. GAO-03-1147T. 2003. <http://www.gao.gov/assets/120/110290.pdf>.

- Unique Identification Authority of India. "Aadhaar Press Release October 2012." October 2012.
- Unique Identity Authority of India. "APNA AADHAAR." June 2013, at p. 6.
- UNODC. "Handbook on Identity-Related Crime 2011." Accessed August 22, 2013. <http://www.unodc.org/unodc/en/organized-crime/tools-and-publications.html>, 118.
- Wang, Tova Andrea. *The Debate Over a National Identification Card*. The Century Foundation Homeland Security Project, May 10, 2002.
- Wasem, Ruth Ellen. *Unauthorized Aliens' Access to Federal Benefits: Policy and Issues*. CRS Report RL34500. Washington, DC: Congressional Research Service, September 17, 2012.
- Whitley, Edgar A. "The Identity Project: An Assessment of the UK Identity Cards Bill and Its Implications." 2005. <http://eprints.lse.ac.uk/29117/>.
- Wikipedia, s.v. "Political Party Strength in Maine." Last modified August 19, 2013. http://en.wikipedia.org/wiki/Political_party_strength_in_Maine.
- Wills, David. "The United Kingdom Identity Card Scheme." In *Playing the Identity Card Surveillance, Security and Identification in Global Perspective*, ed. Colin J Bennett and David Lyon (London; New York: Routledge, 2008), 163.
- Zapotosky, Matt. "IRS Tax Refund Thieves Increasingly Use Stolen Identities to Divert Money to Themselves." *The Washington Post*, sec. Local. February 19, 2014. http://www.washingtonpost.com/local/crime/irs-tax-refund-thieves-increasingly-use-stolen-identities-to-divert-money-to-themselves/2014/02/18/4bd7f4cc-7ed0-11e3-9556-4a4bf7bcbd84_story.html?hpid=z4.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California